PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-173381
(43)Date of publication of application : 20.06.2003

(51)Int.Cl. G06F 17/60
G06F 12/14
G06F 15/00
H04L 9/08
H04L 9/32

(21)Application number : 2002-154341
(22)Date of filing : 28.05.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : DAIHO MASAHIRO
KAMISAKA YASUSHI
YAMAMOTO MASAYA
OKAMOTO RYUICHI
TOKUDA KATSUMI
INOUE MITSUHIRO

(30)Priority

Priority number	Priority date	Priority country
2001160290	29.05.2001	JP
2001224413	25.07.2001	JP
2001291593	25.09.2001	JP

(54) RIGHT TO USE CONTROL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a right to use control device available to use contents data by using own right to use information on another person's equipment.
SOLUTION: Equipment 201 of a contractor γ produces issue request for obtaining the permission of use contents data by using a media identifier inside a portable recording medium 101 of a contractor β and sends it to the right to use control device 71. The right to use control device 71 controls right to use information of the contents data given to the contractor β and produces permission of use information permitting the use of the contents data to the portable recording medium 101 based on the right to use information and the issue request. Furthermorethe right to use

control device 71 produces license information for controlling the use of the contents data in equipment connected to the portable recording mediumbased on the permission to use informationand sends it to the equipment 201. The equipment 201 processes the license information and controls the use of the contents data.

CLAIMS

[Claim(s)]

[Claim 1]Equipment characterized by comprising the following for managing right-of-use information showing a right for two or more apparatus to use contents data.

A right-of-use database including right-of-use information assigned to said two or more apparatus (the right of use DB is called hereafter).

The right-of-use Management Department which generates utilization permission information which shows a utilization permission of contents data to apparatus which transmitted issue requesting using right-of-use information which answers issue requesting from each aforementioned apparatusand is included in said right of use DB.

A license information generation part which generates license information which includes at least utilization permission information generated at said right-of-use Management Department.

The communications department which transmits license information generated by said license information generation part to apparatus which transmitted issue requesting.

[Claim 2]The right-of-use controlling device according to claim 1 which said apparatus transmits a setting request which includes a utilization condition of contents data at leastand said right-of-use Management Department answers a setting request from said apparatusand registers into said right of use DB right-of-use information over apparatus which transmitted a setting request at least.

[Claim 3]The right-of-use controlling device according to claim 2 which said two or more apparatus belongs to a group set beforehandand said right-of-use Management Department answers a setting request from said apparatus of one belonging to said groupand registers into said right of use DB right-of-use information shared by each apparatus belonging to a group.

[Claim 4]The right-of-use controlling device according to claim 2 which is further provided with a send data generation part characterized by comprising the following which generates send data and with which said communications department transmits further data generated by said send data generation part to apparatus which transmitted a setting request.

A contents database which stores contents data used as a distribution object. A contents managing department which it has further (the contents DB are called

hereafter)and a setting request which said apparatus transmits specifies contents data of an acquisition objectanswers a setting request from said apparatus furtherand reads contents data of an acquisition object from the contents DB.
A contents encryption section which enciphers contents data read in said contents managing department.
Contents data enciphered by said contents encryption section.

[Claim 5]A decode key database containing a decode key for decoding contents data enciphered by said contents encryption section. The right-of-use controlling device according to claim 1 which is further provided with (calling the decode key DB hereafter) and with which said license information generation part generates license information which contains further a decode key in said decode key DB.
[Claim 6]The right-of-use controlling device according to claim 5 which is further provided with a decode key encryption section which enciphers a decode key in said decode key DB for information relevant to apparatus which transmitted issue requesting and with which said license information generation part generates license information which contains further a decode key enciphered by said decode key encryption section.
[Claim 7]The right-of-use controlling device comprising according to claim 1:
A hash value generation part which generates a hash value for said license information generation part to prevent an alteration of license information based on utilization permission information generated at said right-of-use Management Department.
A license information assembly part which adds a hash value generated by said hash value generation part to utilization permission information generated at said right-of-use Management Departmentand assembles license information.

[Claim 8]The right-of-use controlling device according to claim 1 with which said right-of-use Management Department generates use refusal information when utilization permission information cannot be generated because of apparatus which becomes transmitting origin of issue requestingand said communications department transmits further use refusal information generated at said right-of-use Management Department to becoming apparatus of transmitting origin of issue requesting.
[Claim 9]The right-of-use controlling device according to claim 1 which answers a registry request characterized by comprising the following from apparatusand is further provided with the User Information Management Department which registers into said User Information DB an unregistered instrument identification child contained in a receiving registry request.
A user information data base which consists of an instrument identification child who specifies each of apparatus belonging to a group set beforehand as a meaning (User Information DB is called hereafter).

An instrument identification child unregistered to said User Information DB.

[Claim 10]When the number of instrument identification children registered into one group is more than upper limit defined beforehandsaid User Information Management DepartmentThe right-of-use controlling device according to claim 9 which answers a registry request and generates a notice of a register reject for refusing registration to said User Information DB and with which said communications department transmits further a notice of a register reject generated at said User Information Management Department to apparatus which becomes transmitting origin of a registry request.
[Claim 11]A user information data base which consists of an instrument identification child who specifies each of apparatus belonging to a group set beforehand as a meaning. Have further (User Information DB is called hereafter)and registered apparatus to said User Information DBA provisional registration demand which contains an own instrument identification child at least as a registering object identifier is transmittedHave further the User Information Management Department which registers provisionally into said User Information DB a registering object identifier contained in a reception provisional registration demandand unregistered apparatus to said User Information DBTransmit and a high-grade-registry demand which contains at least a registering object identifier and a registered identifier which is instrument identification children of apparatus which became transmitting origin of a provisional registration demand said User Information Management DepartmentThe right-of-use controlling device according to claim 1 which carries out high grade registry of the registering object identifier registered provisionally into said User Information DB based on a registering object identifier and a registered identifier which are contained in a receiving high-grade-registry demand.
[Claim 12]The right-of-use controlling device according to claim 1 which transmits a registry request characterized by comprising the following and with which said User Information Management Department does high grade registry of the registering object identifier registered provisionally into said User Information DB based on a password and a registering object identifier which are contained in a receiving registry request.
A user information data base which consists of an instrument identification child who specifies each of apparatus belonging to a group set beforehand as a meaning. Have further (User Information DB is called hereafter)and unregistered apparatus to said User Information DBA password demand which contains an own instrument identification child as a registering object identifierand contains a still more nearly registered instrument identification child is transmittedA registering object identifier contained in a receiving password demand is registered provisionally into said User Information DBit has further the User Information Management Department which publishes a password to still more nearly unregistered apparatusand apparatus unregistered to said User Information DB is a registering object identifier.

A password published by said User Information Management Department.

[Claim 13]A user information data base which consists of an instrument identification child who specifies each of apparatus belonging to a group set beforehand as a meaning. Have further (User Information DB is called hereafter)and unregistered apparatus to said User Information DBTransmit to apparatus registered to User Information DBand the 1st registry request that contains an own instrument identification child at least as a registering object identifier registered apparatus to said User Information DBThe 2nd registry request containing a registering object identifier contained in the 1st registry request further received including an own instrument identification child as a registered identifier is transmittedThe right-of-use controlling device according to claim 1 further provided with the User Information Management Department which registers a registering object identifier contained in the 2nd received registry request into said User Information DB.
[Claim 14]An instrument identification child of available apparatus is registered into said right of use DB in right-of-use information and its right-of-use information.
A user information data base (User Information DB is called hereafter) which consists of an instrument identification child who specifies each of apparatus belonging to a group set beforehand as a meaningThe right-of-use controlling device according to claim 1 which answers a deletion request from each aforementioned apparatusand is further provided with an instrument identification child cutout which deletes an instrument identification child from said User Information DB and said right of use DB.

[Claim 15]Said two or more apparatus belongs to a group set beforehandand said right-of-use Management DepartmentAnswer a setting request from the 1st apparatus belonging to said groupand register into said right of use DB right-of-use information on the 1st apparatus that becomes transmitting origin of a setting requestand a setting request from the 2nd apparatus belonging to said group is answeredThe right-of-use controlling device according to claim 2 which registers into said right of use DB the 2nd apparatus that becomes transmitting origin of a setting request so that right-of-use information on the 1st apparatus and a share are possible.
[Claim 16]From a right-of-use controlling device connected through a transmission lineare offer of license information apparatus which wins popularityand said apparatusInterface Division which connects a portability type recording medium which stores a media identifier which specifies self as a meaning so that data communications are possibleAn identifier extraction part which takes out a media identifier from a portability type recording medium connected to said Interface DivisionAn issue requesting generation part which generates issue requesting required in order to obtain a utilization permission of contents data using a media identifier received from said identifier extraction partHave the 1st communications department

which transmits issue requesting received from said issue requesting generation part to said right-of-use controlling device through said transmission lineand said right-of-use controlling deviceHave managed right-of-use information on contents data given to said portability type recording mediumand issue requesting from said apparatus is answeredGenerate license information for controlling use of contents data in apparatus to which said portability type recording medium was connectedtransmitand said apparatus processes license information from said right-of-use controlling device furtherApparatus provided with a license information treating part which controls use of contents data.

[Claim 17]The apparatus according to claim 16 by which said right-of-use controlling device is provided with the right-of-use Management Department which generates utilization permission information at its minimum for said apparatus to use contents data.

[Claim 18]The 1st hash value generation part that generates the 1st hash value based on utilization permission information generated at said right-of-use Management Department in order that said right-of-use controlling device may generate license informationThe apparatus according to claim 17 which adds the 1st hash value received from said 1st hash value generation part to utilization permission information received from said right-of-use Management Departmentand contains a license information assembly part which assembles license information.

[Claim 19]The 2nd hash value generation part that generates the 2nd hash value based on utilization permission information by which said license information treating part is contained in receiving license informationThe 1st hash value contained in license information received from said 1st communications departmentThe apparatus according to claim 18 containing an alteration judgment part which judges whether utilization permission information included in license information received from said 1st communications department is altered based on the 2nd hash value received from said 2nd hash value generation part.

[Claim 20]Said contents data is distributed in the state where it was enciphered with an encryption key beforehand provided in said apparatusSaid license information assembly part takes out a media identifier from issue requesting received from said right-of-use Management Department furtherand said right-of-use controlling deviceThe decode key Management Department which manages a decode key which can decode contents data enciphered with said encryption keyIt has further a decode key encryption section which enciphers a decode key managed at said decode key Management Department by a media identifier taken out by said license information assembly partThe apparatus according to claim 18 which said license information assembly part adds an enciphered decode key which is received from said decode key encryption section to utilization permission information received from said right-of-use Management Department furtherand assembles license information.

[Claim 21]The apparatus according to claim 20 further provided with a decode key

decoding part which decodes an enciphered decode key which is contained in license information received from said 1st communications department using a media identifier which said license information treating part receives from said identifier extraction part.

[Claim 22]Have further an instrument identification child storage for storing an instrument identification child assigned to selfand said identifier extraction partThe apparatus according to claim 16 which determines whether to take out a media identifier from a portability type recording medium connected to said Interface Division according to a user's operationor take out an instrument identification child from said instrument identification child storage.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]More specificallythis invention relates to the right-of-use controlling device which manages the right relevant to contents data about a right-of-use controlling device.

[0002]

[Description of the Prior Art]In recent yearsa contents distribution system is broadband-izing and always [network] becoming familiar according to connection environment. Since protection of the right relevant to contents data is importantresearch and development of various right management technology are made from the former by the spread of such contents distribution systems. Herein Description of this applicationthe right relevant to contents data like copyright or dealership is called digital rights. Hereafterthe contents information distribution system incorporating the conventional right management technology is explained.

[0003]By the network represented by the Interneta content distribution device and a personal computer (it is hereafter written as PC) are connected to the conventional contents distribution system so that data communications are possible. The content distribution device stores at least one **** of contents dataa contents decode keyand utilization condition data. Contents data is digital data which expresses the contents represented by musicfor example.

It is enciphered by the system defined beforehand.

A contents decode key is a key for decoding the enciphered contents data. Utilization condition data is data showing the available conditions (a utilization condition is called hereafter) of above-mentioned contents data. As a utilization conditionthe using frequency of contents data is typical. PC stores the computer program (a program is only called hereafter) required in order to use the contents data which acquired above-mentioned contents data from the content distribution deviceand acquired it

further.
[0004]In the above contents distribution systemcontents data is distributed as follows. FirstPC executes the program stored beforehand and requires distribution of contents data of a content distribution device. The demand of contents data is generally performed because PC transmits contents specific information and terminal inherent information to a content distribution device via a network. Contents specific information is information which specifies above-mentioned contents data as a meaning. Terminal inherent information is beforehand held with PC.
It is the information which can be specified as a meaning about PC which is the demand origin of above-mentioned contents data.

[0005]A content distribution device answers the demand from PCand enciphers an above-mentioned contents decode key using the terminal inherent information received this time. Thena content distribution device transmits the enciphered above-mentioned contents datathe contents decode key enciphered by terminal inherent informationand utilization condition data to PC. PC receives the contents datathe contents decode keyand utilization condition data which were distributed by the content distribution deviceand stores them in the memory storage with which an inside is equipped.
[0006]After the above storingthe user of PC is decoding contents data and will be in the state in which an output of the contents which it expresses is possible. By the time it actually outputs contentsa user will direct that to PC first. Answering these directionsthe PC operates as follows. PC judges whether this use has agreed in the utilization condition expressed by the utilization condition data in memory storage. PC is restricted when agreeing in a utilization conditionand it performs the following processings. Nextsince the contents decode key in memory storage is encipheredPC decodes the contents decode key concerned using the terminal inherent information which self holds. Since the contents data in memory storage is also enciphered as mentioned abovePC reproduces and outputs the contents which it expressesafter decoding the contents data concerned using the decoded contents decode key.
[0007]Digital rights are protected in the above contents distribution system by DRM (DigitalRights Management) as right management technology. Protection of the digital rights by DRM is realized by the following three technology. In the 1st protection techniquea content distribution device transmits the contents decode key enciphered as the enciphered contents data by terminal inherent information. Herea contents decode key cannot be decoded except PC which required contents data. Soeven if the enciphered contents data is transmitted to other PCsother PCs cannot solve the code of a contents decode keyandas a resultcannot reproduce contents data. From the above thingit can be said by DRM that a contents decode key is fastened to the only PC. Therebydigital rights are protected.
[0008]The 2nd protection technique is the Tampa-proof technology. That isalthough

the decoding program for solving each code is needed for PCthe analysis of the decoding program concerned is prevented by the above-mentioned Tampa-proof technology. Digital rights are protected by this.
[0009]As mentioned above to the 3rdin the conventional contents distribution systema content distribution device transmits utilization condition data to PC. PC manages the received utilization condition data. And PC does not perform processing after itwhen the utilization condition which the utilization condition data which self manages expresses is checked for every use of contents data and this use has not agreed in a utilization condition. Digital rights are protected by this.
[0010]
[Problem to be solved by the invention]In recent yearsa network connection function has come to be added also to household equipments other than PC represented by a set top boxa television receivera music reproduction machineand the game machine machine. By thiscontents data can be received now from the content distribution device with an above-mentioned household equipmentand data communications have become possible among further two or more household equipments. From the above thingright management technology is wanted to be included also in a household equipment. Howeversince the following problems can be assumedit is not a best policy to include right management technology like above-mentioned DRM in a household equipment.
[0011]Since a contents decode key was fastened to the 1st by the only PCeven if the user of PC and other household equipments was the sameother household equipments had the problem that contents data could not be decodedusing the contents decode key. When a user uses contents data because of such a problemin order to have to use PC which can use a contents keythe conventional right management technology was not user-friendly for the user.
[0012]Before the Tampa-proof technology is included in the 2nd by above-mentioned DRM and PC reproduces contents data furtherbased on the utilization condition data stored in the insideit is certainly confirmed whether it is available in the contents data concerned. Thusthe Tampa-proof technology forces above-mentioned PC a big processing burden. HoweverPC mounts highly efficient hardware relativelyfor example so that it can use for general-purpose usessuch as video recoveryaudio reproductionor a game play. Soalthough DRM is included in PCit does not become a problem so much. A household equipment is asked a low price from itandas for a household equipmentit is still more common to be used for the use which specialized in each of video recoveryaudio reproductionand a game play. From the above viewpointhighly efficient hardware was not mounted in the household equipmentbut there was a problem that it was difficult to incorporate DRM which requires a big processing burden in it as PC.
[0013]Sothe 1st purpose of this invention is to provide the right management technology in which digital rights with two or more common household equipments are

sharable. The 2nd purpose of this invention is to provide right management technology suitable for a household equipment.
[0014]
[The means for solving a technical problem and an effect of the invention] In order to attain the 1st purpose of the aboveinvention of the 1st of an application concernedA right-of-use database (the right of use DB is called hereafter) including the right-of-use information by which two or more apparatus is equipment for managing the right-of-use information showing the right for using contents dataand is assigned to two or more apparatusThe right-of-use Management Department which generates the utilization permission information which shows the utilization permission of the contents data to the apparatus which transmitted issue requesting using the right-of-use information which answers the issue requesting from each apparatus and is included in the right of use DBIt has a license information generation part which generates the license information which includes at least the utilization permission information generated at the right-of-use Management Departmentand the communications department which transmits the license information generated by the license information generation part to the apparatus which transmitted issue requesting.
[0015]As mentioned aboveaccording to the 1st inventionsince right-of-use information is assigned to two or more apparatusit becomes possible to provide the right protection technology in which the right-of-use information that two or more apparatus is common is sharable.
[0016]In order to attain the 2nd purpose of the aboveinvention of the 2nd of an application concerned is provided with the following.
Interface Division whose apparatus are apparatus which receives offer of license informationthe portability type recording medium stores the media identifier which specifies self as a meaningand connects a portability type recording medium from the right-of-use controlling device connected through the transmission line so that data communications are possible.
The identifier extraction part which takes out a media identifier from the portability type recording medium connected to Interface Division.
The issue requesting generation part which generates issue requesting required in order to obtain the utilization permission of contents data using the media identifier received from an identifier extraction part.
The 1st communications department which transmits the issue requesting received from an issue requesting generation part to a right-of-use controlling device through a transmission line.
Herethe right-of-use controlling device has managed the right-of-use information on the contents data given to the portability type recording mediumanswers the issue requesting from apparatusgenerates the license information for controlling use of the contents data in the apparatus to which the portability type recording medium was

connectedand transmits. Furtherapparatus processes the license information from a right-of-use controlling deviceand is provided with the license information treating part which controls use of contents data.
[0017]Since the right-of-use information on contents data is managed by the right-of-use controlling device side as mentioned above according to the 2nd inventionthe necessity of burdening with the processing burden which starts apparatus for right-of-use information is lost. It becomes possible to provide the right protection technology which was relatively suitable for the low apparatus of throughput by this.
[0018]According to the 2nd inventionin apparatusan identifier extraction part takes out a media identifier from a portability type recording medium connected to apparatus. The issue requesting generation part can generate issue requesting using a taken-out media identifier. By thisa user of a portability type recording medium becomes possible [using contents data on the others' apparatus] using his right-of-use information.
[0019]
[Mode for carrying out the invention]"1st embodiment" drawing 1 is a block diagram showing an entire configuration of the license information managerial system Sa which accommodated the right-of-use controlling device 11 concerning a 1st embodiment of this invention. The license information managerial system Sa is provided with the following in drawing 1.
The right-of-use controlling device 11.
It is the two apparatus 21a and 21b as an example of two or more apparatus 21.
The transmission line 31.
The right-of-use controlling device 11 is installed in the entrepreneur alpha side in connection with contents distribution. Typicallythe apparatus 21a and 21b is used by the contractor beta who receives contents distribution based on a contract with the entrepreneur alpha. The transmission line 31 is a cable or radioand connects the right-of-use controlling device 11and the apparatus 21a or the apparatus 21b so that data communications are possible.
[0020]Nextwith reference to drawing 2detailed composition of the right-of-use controlling device 11 of drawing 1 is explained. In drawing 2the right-of-use controlling device 11 is provided with the following.
The contents database 111.
The decode key database 112.
The user information data base 113.
The right-of-use database 114the communications department 115the user authentication part 116the right-of-use Management Department 117the contents managing department 118the contents encryption section 119the send data generation part 120the license information generation part 121the decode key Management Department 122and the decode key encryption section 123.
In more detailthe license information generation part 121 contains the hash value

generation part 1211 and the license information assembly part 1212as shown in drawing 3.
[0021]Nextwith reference to drawing 4detailed composition of the apparatus 21a and 21b of drawing 1 is explained. Typically in drawing 4the apparatus 21a and 21b is either a personal computer (PC is called hereafter)a set top boxa music reproduction machinea television receiver and a game machine. Howeverin this embodimentit is assumed for convenience that the apparatus 21a and 21b is PC and a music reproduction machine with which each has a music reproduction function. Under this assumptionat least each of the apparatus 21a and 21b The instrument identification child storage 211It has the setting request generation part 212the communications department 213the contents managing department 214the contents accumulating part 215the issue requesting generation part 216the license information treating part 217the contents decoding part 218and the contents reproduction part 219. In more detailthe license information treating part 217 contains the alteration judgment part 2171the hash value generation part 2172the utilization permission judgment part 2173and the decode key decoding part 2174as shown in drawing 5.
[0022]Nextin the above-mentioned license information managerial system Sapreparation which is needed in order that the contractor beta may receive contents distribution from the entrepreneur alpha is explained. In this preparatory workthe contents database (the contents DB are called hereafter) 111 of drawing 2the decode key database (the decode key DB is called hereafter) 112and the user information data base (User Information DB is called hereafter) 113 are built by the entrepreneur alpha.
[0023]Firstwith reference to drawing 6 (a)contents DB111 of drawing 2 is explained in detail. Firstthe entrepreneur alpha creates by himself the contents data Dcnt distributed to the contractor betaor receives it from another content producer. Herethe contents data Dcnt is data available by both apparatus 21a and 21bfor exampleexpresses a TV programa moviea radio programmusicbooksor printed matter. The contents data Dcnt may be a game program or application software. Howeverby this embodimentit is assumed for convenience that the contents data Dcnt is data showing music.
[0024]The entrepreneur alpha assigns each of the contents data Dcnt obtained as mentioned above content identifier Icnt. Content identifier Icnt is information which specifies the contents data Dcnt as a meaning in this license information managerial system Sa preferably. As for content identifier Icntit is preferred that it is also a locator which shows the storing position of the contents data Dcnt. The above contents data Dcnt is distributed to the apparatus 21a or 21b from a viewpoint of protecting digital rightsin the state where it was enciphered by the right-of-use controlling device 11 side. Thereforethe entrepreneur alpha assigns the encryption key Ke for exclusive use to each contents data Dcnt. The combination of content identifier Icnt of a more thanthe contents data Dcntand the encryption key Ke is

accumulated in contents DB111. Thereforeas shown in drawing 6 (a)contents DB111 becomes a meeting of the combination of content identifier Icntthe contents data Dcntand the encryption key Ke. In contents DB111content identifier Icnt specifies the same group Mino contents data Dcnt as a meaning especially. The encryption key Ke is used in order to encipher the same group Mino contents data Dcnt.

[0025]By this embodimentin order that a graphic display may simplifyit is explained that contents DB111 comprises content identifier Icntthe contents data Dcntand the encryption key Kebut the contents data Dcnt and a database for every encryption key Ke may be built. As for content identifier Icntit is preferred that it is a locator of the contents data Dcnt. In such a casesince the right-of-use controlling device 11 can read the contents data Dcnt from contents DB111 using content identifier Icnt contained in the setting request Drra of the apparatus 21a or 21bThere is no necessity of registering content identifier Icnt into contents DB111.

[0026]Nextwith reference to drawing 6 (b)decode key DB112 of drawing 2 is explained in detail. As mentioned aboveeach contents data Dcnt is transmitted to the apparatus 21a or 21b in the state where it was enciphered with the encryption key Ke. Herein the following explanationthe contents data Dcnt enciphered with the encryption key Ke is called the code finishing contents data Decnt. For decoding of the code finishing contents data Decntthe apparatus 21a or 21b needs to be provided with the decode key Kd corresponding to the encryption key Ke. From this necessitythe entrepreneur alpha prepares the decode key Kd corresponding to each encryption key Ke in the contents DB111. Herethe decode key Kd may consist of the same bit string as the encryption key Keand may consist of a different bit string. The above decode key Kd is registered into decode key DB112 with above-mentioned content identifier Icnt. Decode key DB112 becomes a meeting of combination of content identifier Icnt and the decode key Kd from the above thingas shown in drawing 6 (b). In decode key DB112content identifier Icnt specifies the contents data Dcnt currently especially assigned to the same decode key Kd to construct. The decode key Kd is used in order to decode the code finishing contents data Decnt specified by the same group Mino content identifier Icnt.

[0027]Nextwith reference to drawing 7 (a)User Information DB113 of drawing 2 is explained in detail. As mentioned abovethe contractor beta signs a contract concerning the entrepreneur alpha and contents distribution. Hereabout both contractthe contractor beta may carry out with the entrepreneur alpha through the transmission line 31and it may carry out with other forms. Based on this contractthe entrepreneur alpha assigns each of two or more apparatus 21 (getting it blocked apparatus 21a and 21b) which the contractor beta owns the instrument identification child Idv. Hereby this embodimentas shown in drawing 1since the apparatus 21a and 21b is illustratedthe entrepreneur alpha assigns the instrument identification children Idva and Idvb as each instrument identification child Idv. The instrument identification children Idva and Idvb specify the apparatus 21a and 21b by the side of the

contractor beta as a meaning in the license information managerial system Sa. The above instrument identification children Idva and Idvb are registered into User Information DB113. Even if the contractor beta and its authorized personnel use any of the apparatus 21a and 21bthe entrepreneur alpha assigns the group identification descriptor Igp to a contract with the contractor beta so that the contents data Dcnt can be used. Herethese are called the user beta so that the contractor beta and its authorized personnel can be described comprehensively. The entrepreneur alpha builds User Information DB113 using the above instrument identification children Idva and Idvb and group identification descriptor Igp.

[0028]More specificallyUser Information DB113 is a meeting of two or more contractor records Rcsas shown in drawing 7 (a). The contractor record Rcs is provided with the following.

It is created for every contract andtypicallyis the group identification descriptor Igp.

The number Ndv of instrument identification children.

Two or more instrument identification children Idv.

The group identification descriptor Igp specifies that two or more instrument identification children Idv contained in the contractor record Rcs belong to the same group. The number Ndv of instrument identification children shows the number of the apparatus 21 belonging to a group specified by the group identification descriptor Igp. Each instrument identification child Idv specifies each apparatus 21 belonging to a group specified by the group identification descriptor Igp. With the above contractor record Rcsthe right-of-use controlling device 11 can grasp that two or more apparatus 21 belongs to the same group. When a contractor uses one set only of the apparatus 21the contractor record Rcs should contain only the instrument identification child Idv assigned to it.

[0029]Drawing 4 is referred to again here. The instrument identification children Idva and Idvb assigned by the entrepreneur alpha are further set as the instrument identification child storage 211 in the users' beta apparatus 21a and 21b. Although the instrument identification children's Idva and Idvb both sides seem to be stored in the instrument identification child storage 211 in drawing 4 as for requiring cautions hereThat is not rightthe instrument identification child Idva is set to the instrument identification child storage 211 of the apparatus 21aand the instrument identification child Idvb is set to the instrument identification child storage 211 of the apparatus 21b. About the above instrument identification children's Idva and Idvb setting outthe entrepreneur alpha operates and sets up the users' beta apparatus 21a or 21bfor example. Otherwisethe entrepreneur alpha side transmits the instrument identification children Idva and Idvb who assigned the contractor beta to the apparatus 21a or 21b through the transmission line 31It may be made for each to set the instrument identification children Idva and Idvb who received as each instrument identification child storage 211 automatically. The above instrument identification children Idva and Idvb may be set as each instrument identification child storage 211 at the time of

factory shipments of the apparatus 21a or 21b. In such a casethe contractor beta notifies the entrepreneur alpha of the instrument identification children Idva and Idvb set as the apparatus 21a and 21b at the time of a contract. The entrepreneur alpha builds User Information DB113 using the instrument identification children Idva and Idvb of whom it was notified.

[0030]Although the right-of-use database 114 is shown in drawing 7 (b)this is mentioned later.

[0031]After the above preparation is completedone side of the apparatus 21a and 21b becomes possible [setting up the right of use of the contents data Dcntor acquiring the contents data Dcnt] to the right-of-use controlling device 11 according to the user's beta operation. Hereafterdrawing 8 is referred to and data communications between the apparatus 21a at the time of right-of-use setting out of the contents data Dcnt and acquisition and the right-of-use controlling device 11 are explained. Firstthe user beta operates the apparatus 21aaccesses the right-of-use controlling device 11and specifies content identifier Icnt of a thing to acquire this time from the contents data Dcnt in the contents DB111. In subsequent explanationthe contents data Dcnt specified this time is called the acquisition object contents data Dcnt. The user beta specifies the utilization condition Ccnt at the time of using the acquisition object contents data Dcnt.

[0032]Hereafterthe utilization condition Ccnt is explained more to details. What kind of conditions are the utilization conditions Ccntand are information which shows whether the apparatus 21a requires setting out of the right of use of the contents data Dcnt. When the contents data Dcnt expresses musicas the utilization condition Ccnta shelf-lifereproduction frequencythe maximum continuous reproduction timetotal reproduction timeor quality of a recycled article is typical. The utilization conditions Ccnt may be two or more combination among a shelf-lifereproduction frequencythe maximum continuous reproduction timetotal reproduction timeand quality of a recycled article. For example a shelf-life as the utilization condition Ccnt is set to June 12001 to August 312001and is restricted to a set-up periodand the apparatus 21a can reproduce the contents data Dcnt. For example reproduction frequency is set to 5 timesand is restricted to the set-up number of timesand the apparatus 21a can reproduce the contents data Dcnt. If the maximum continuous reproduction time is till time which was set to 10 seconds and set up in one reproductionfor examplethe apparatus 21a can reproduce the contents data Dcnt. Such maximum continuous reproduction time especially is effective in a musical promotion. Total reproduction time is set to 10 hoursfor exampleand if it is within the limits of set-up timethe apparatus 21a can reproduce the contents data Dcnt freely. Quality of a recycled article is set to quality of CD (Compact Disc)for exampleand the apparatus 21a can play the contents data Dcnt qualitatively of a recycled article which was set up.

[0033]The utilization condition Ccnt which it is set up when the contents data Dcnt

expresses musicand is sold at **** was explained. Howeveras for **** and the utilization condition Ccntit is preferred to be appropriately set up according to the contents which the contents data Dcnt expresses. For convenienceby this embodimentthe following explanation is continued noting that the utilization condition Ccnt is the reproduction frequency of the contents data Dcnt.

[0034]As mentioned abovethe user beta operates the apparatus 21a and specifies content identifier Icnt and the utilization condition Ccnt. Answering this specificationthe apparatus 21a generates the setting request Drra shown in drawing 9 (a)and transmits to the right-of-use controlling device 11 (drawing 8; Step S11). Although the setting request Drra is the information for requiring right-of-use setting out of the acquisition object contents data Dcnt of the right-of-use controlling device 11in this embodimentit is also the information for requiring distribution of the acquisition object contents data Dcnt of the right-of-use controlling device 11 further. If Step S11 is explained more concretelythe setting request generation part 212 (refer to drawing 4) will receive content identifier Icnt and the utilization condition Ccnt specified by the user beta first. The setting request generation part 212 receives the instrument identification child Idva from the instrument identification child storage 211. Thenthe setting request generation part 212 adds the setting request identifier Irr held beforehand to the above instrument identification child Idvacontent identifier Icntand utilization condition Ccntand generates the setting request Drra (refer to drawing 9 (a)). Heresince the right-of-use controlling device 11 specifies the setting request Drrathe setting request identifier Irr is used. The setting request generation part 212 passes the communications department 213 the above setting request Drra. The communications department 213 transmits the received setting request Drra to the right-of-use controlling device 11 through the transmission line 31.

[0035]In the right-of-use controlling device 11 (refer to drawing 2)the communications department 115 receives the setting request Drra transmitted through the transmission line 31and hands the user authentication part 116. The user authentication part 116 will perform user authentication processing for judging whether the apparatus 21a of the transmitting origin is a thing of contract user betaif the setting request Drra is received (drawing 8; Step S12). More specificallythe user authentication part 116 checks whether above-mentioned User Information DB113 (refer to drawing 7 (a)) is accessedand the match is registered into the User Information DB113 concerned by the instrument identification child Idva in the received setting request Drra. The user authentication part 116 is restricted when the match is registered into User Information DB113and it attests with the setting request Drra being transmitted from the user's beta apparatus 21 this time. The user authentication part 116 passes the right-of-use Management Department 117 the received setting request Drraafter the above user authentication is completed.

[0036]When the setting request Drra from other than contract user beta is receivedthe user authentication part 116 fails in user authentication. In this casethe

user authentication part 116 is discardedwithout passing the right-of-use Management Department 117 the reception setting demand Drra.
[0037]The right-of-use Management Department 117 is judging the setting request identifier Irr set as receipt information from the user authentication part 116and recognizes that this receipt information is the setting request Drra. According to this recognition resultthe right-of-use Management Department 117 (refer to drawing 2) accesses the right-of-use database (the right of use DB is called hereafter) 114and performs right-of-use registration processing of right-of-use DB114 (Step S13). More specificallythe right-of-use Management Department 117 judges whether the instrument identification child Idva and content identifier Icnt are taken out from the reception setting demand Drraand the right-of-use record Rrgt containing these is registered into right-of-use DB114 (refer to drawing 7 (b)) (Step S131). If it assumes that the target right-of-use record Rrgt is unregistered to right-of-use DB114 nowthe right-of-use Management Department 117 will perform Step S132. At Step S131about operation when the right-of-use record Rrgt is registeredin order to explain with operation of the apparatus 21bthe explanation is omitted here.
[0038]In Step S132firstthe right-of-use Management Department 117 accesses User Information DB113 (refer to drawing 7 (a))after taking out the instrument identification child Idvacontent identifier Icntand the utilization condition Ccnt from the reception setting demand Drra. And the right-of-use Management Department 117 takes out the group identification descriptor Igp and all the instrument identification children Idva and Idvb from the contractor record Rcs including the instrument identification child Idva who took out this time (Step S132). Nextthe instrument identification child Idvacontent identifier Icntand the utilization condition Ccnt which the right-of-use Management Department 117 took out from the reception setting demand Drra. Combination with the group identification descriptor Igp and the instrument identification children Idva and Idvb who got from User Information DB113 is registered into right-of-use DB114 as the right-of-use record Rrgt (Step S133). Herethe right-of-use Management Department 117 considers that grant of a right for the apparatus 21a to use the acquisition object contents data Dcnt by the utilization condition Ccnt in the setting request Drra is demanded. From the above thingthe right-of-use Management Department 117 treats the utilization condition Ccnt taken out from the setting request Drra as the right-of-use information Drgt. That isthe right-of-use information Drgt shows a right for the apparatus 21a to use the contents data Dcntunder conditions which the utilization condition Ccnt shows.
[0039]By the above registration processingright-of-use DB114 becomes a meeting of the right-of-use record Rrgt including group identification descriptor Igpthe instrument identification children Idva and Idvbcontent identifier Icntand the right-of-use information Drgtas shown in drawing 7 (b). By thisthe right-of-use Management Department 117 manages the right of use for every acquisition object contents data Dcnt of the contractor beta. By what one feature of this embodiment carries out and

all the instrument identification children Idva and Idvb who got from User Information DB113 on the right-of-use record Rrgt are added for. By the setting request Drra from the apparatus 21athe apparatus 21a and 21b can share now the right of use of the contents data Dcnt. The right-of-use Management Department 117 hands the setting request Drra received this time to the contents managing department 118after the above utilization condition registration processing is completed.

[0040]When it assumes that "m playbacks" (m is a natural number) is set up as the utilization condition Ccntas shown in drawing 7 (b)the right-of-use record Rrgt by which new registration is carried out this time will include the right-of-use information Drgt as which the conditions of "m playbacks" were specified in this setting request Drra.

[0041]Although it is not related to the technical feature of this license information managerial system Sain Step S13 the right-of-use Management Department 117Fee collection to use of the contents data Dcnt may be performed for the contractor beta to whom the instrument identification child Idva is assigned for every registration of the utilization condition information Dcrt.

[0042]The contents managing department 118 will perform reading processing of the contents data Dcnt and the encryption key Ke of its exclusive useif the setting request Drra is received (Step S14). More specificallythe contents managing department 118 takes out content identifier Icnt from the reception setting demand Drra. Thenthe contents managing department 118 reads the contents data Dcnt to which contents DB111 is accessed and taken-out content identifier Icnt is assignedand the encryption key Ke. After the above reading processing is completedthe contents managing department 118 passes the read contents data Dcnt and the encryption key Ke to the contents encryption section 119. The contents managing department 118 passes the received setting request Drra to the send data generation part 120.

[0043]The contents encryption section 119 performs cipher processing of the contents data Dcnt (Step S15). The contents encryption section 119 enciphers the received contents data Dcnt with the encryption key Ke received simultaneouslyandmore specificallygenerates the above-mentioned code finishing contents data Decnt. The contents encryption section 119 passes the code finishing contents data Decnt to the send data generation part 120after the above cipher processing is completed.

[0044]The send data generation part 120 will perform send data generation processingif the code finishing contents data Decnt from the setting request Drra and the contents encryption section 119 from the contents managing department 118 is assembled (Step S16). More specificallythe send data generation part 120 takes out content identifier Icnt and the instrument identification child Idva from the reception setting demand Drra. The send data generation part 120 adds the instrument identification child Idva and content identifier Icnt which were taken out to the

received code finishing contents data Decntand generates send data Dtrna as shown in drawing 9 (b). The send data generation part 120 passes the communications department 115 send data Dtrnaafter the above send data generation processing is completed. The communications department 115 transmits received send data Dtrna to the apparatus 21a via the transmission line 31 (Step S17).

[0045]In the apparatus 21a (refer to drawing 4)the communications department 213 receives send data Dtrna transmitted through the transmission line 31 (Step S18). More specificallythe communications department 213 recognizes having received this time send data Dtrna addressed to oneself containing the acquisition object contents data Dcnt from the instrument identification child Idva and content identifier Icnt which are contained in it. According to such a recognition resultthe communications department 213 hands received-data Dtrna to the contents managing department 214.

[0046]The contents managing department 214 stores content identifier Icnt in received-data Dtrnaand the code finishing contents data Decnt in the contents accumulating part 215 (Step S19). That isas shown in drawing 10some content identifier Icnt(s) demanded using the above-mentioned setting request Drra and **** of the code finishing contents data Decnt will be accumulated in the contents accumulating part 215.

[0047]From a viewpoint of protection of digital rightsthe code finishing contents data Decnt is distributed to the apparatus 21a. Thereforewhen using the contents data Dcntthe apparatus 21a is the decode key Kd provided by the right-of-use controlling device 11and needs to decode the code finishing contents data Decnt. Herein this license information managerial system Sain order to provide the apparatus 21a with the decode key Kdlicense information Dlca is used. Hereafterdrawing 11 - drawing 13 are referred toand operation of the apparatus 21a at the time of acquisition of license information Dlca and decoding of the contents data Dcnt and the right-of-use controlling device 11 is explained.

[0048]Firstthe user beta operates the apparatus 21a and specifies a thing to use this time out of the code finishing contents data Decnt stored in the contents accumulating part 215. Herein the following explanationthe code finishing contents data Decnt specified this time is called the decoding object contents data Decnt. Answering specification by the user betathe apparatus 21a generates the issue requesting Dira as shown in drawing 14 (a)and transmits to the right-of-use controlling device 11 (drawing 11; Step S21). The issue requesting Dira is information for the apparatus 21a to require issue of above-mentioned license information Dlca of the right-of-use controlling device 11. The contents managing department 214 (refer to drawing 4) takes out content identifier Icnt added to the decoding object contents data Decnt specified by the contractor beta from the contents accumulating part 215andmore specificallypasses it to the issue requesting generation part 216. The issue requesting generation part 216 receives content identifier Icnt taken out by the contents managing department 214. The issue requesting generation part 216 takes

out the instrument identification child Idva from the instrument identification child storage 211. Thenthe issue requesting generation part 216 adds the issue requesting identifier Iir to combination of the instrument identification child Idva and content identifier Icntand generates the issue requesting Dira (refer to drawing 14 (a)). Heresince the right-of-use controlling device 11 specifies the issue requesting Dirathe issue requesting identifier Iir is used. The issue requesting generation part 216 passes the communications department 213 the above issue requesting Dira. The communications department 213 transmits the received issue requesting Dira to the right-of-use controlling device 11 through the transmission line 31.

[0049]In the right-of-use controlling device 11the communications department 115 (refer to drawing 2) receives the issue requesting Dira transmitted through the transmission line 31and hands the user authentication part 116. The user authentication part 116 will perform user authentication processingif the issue requesting Dira is received (Step S22). Since user authentication in Step S22 is the same as that of it of Step S12detailed explanation is omitted. The user authentication part 116 is restricted when it succeeds in user authenticationand it passes the right-of-use Management Department 117 the receiving issue requesting Dira.

[0050]The right-of-use Management Department 117 checks the issue requesting identifier Iir set as itand recognizes that it is the issue requesting Dira which was passed from the user authentication part 116. According to this recognition resultthe right-of-use Management Department 117 takes out the instrument identification child Idva and content identifier Icnt from the received issue requesting Dira (Step S23). Nextthe right-of-use Management Department 117 judges whether the right-of-use record Rrgt containing the instrument identification child Idva who took outand the same thing as combination of content identifier Icnt is registered into right-of-use DB114 (refer to drawing 7 (b)) (Step S24).

[0051]The right-of-use Management Department 117 refers to the right-of-use information Drgt included in the target right-of-use record Rrgtwhen it is judged as "Yes" at Step S24It is judged whether the right of use of whether a utilization permission can be given to the apparatus 21a and the contents data Dcnt that isremains (Step S25). When it is judged as "Yes" at Step S25the right-of-use Management Department 117 generates the utilization permission information Dlwa with reference to the target right-of-use information Drgt (Step S26). The utilization permission information Dlwa is information for giving decoding permission of the decoding object contents data Decnt to the apparatus 21a. By generation of the utilization permission information Dlwasince the right-of-use information Drgt on the apparatus 21a will be usedit is Step S26next only the part for which the right-of-use Management Department 117 was used at Step S26 updates the right-of-use information Drgt (Step S27). It is an execution-time point of Step S27and when all the right-of-use information Drgt is usedthe right-of-use record Rrgt having contained it may be deleted from right-of-use DB114.

[0052]Herethe example of processing of the above steps S25-S27 is explained. If an above-mentioned assumption is followedin the target right-of-use record Rrgtthe right-of-use information Drgt expresses this time the right of use "m playbacks"as shown in drawing 7 (b). Thereforein Step S25the right-of-use Management Department 117 judges that the reproducing permission of the decoding object contents data Decnt may be given to the apparatus 21a. According to this judgmentthe right-of-use Management Department 117 is Step S26and creates the utilization permission information Dlwa. As the utilization permission information Dlwa generated at this timen reproductionis mentionedfor example. Heren is a natural number which does not exceed above-mentioned mfor exampleis the value which the user beta operated the apparatus 21a and specified. As othersn may be set by the right-of-use Management Department 117 side according to the throughput of the apparatus 21a. Step S26 will use the right for the apparatus 21a to reproduce the decoding object contents data Decntn times. Thereforein Step S27the right-of-use Management Department 117 updates the right-of-use information Drgt in a "reproduction (m-n) time" from "m reproduction."

[0053]Although explained in the above example that the right-of-use information Drgt was the reproduction frequency of the contents data Dcntvarious right-of-use information Drgt (that isutilization condition Ccnt) can be set up with this license information managerial system Sa to have mentioned above. Thereforeprocedure from Step S23 to S27 needs to be appropriately specified according to the right-of-use information Drgt.

[0054]The right-of-use Management Department 117 (refer to drawing 2) hands the above utilization permission information Dlwa to the license information generation part 121 together with the issue requesting Dira. More specificallythe license information generation part 121 contains the hash value generation part 1211 and the license information assembly part 1212as shown in drawing 3. The utilization permission information Dlwa is passed to the hash value generation part 1211and both sides of the utilization permission information Dlwa and the issue requesting Dira are passed to the license information assembly part 1212.

[0055]Firstthe hash value generation part 1211 substitutes the received utilization permission information Dlwa for hash function f(x) held beforehandand generates hash value Vhsa for carrying out which prevents an alteration of the utilization permission information Dlwa (Step S28). That ishash value Vhsa is a solution acquired when the utilization permission information Dlwa is substituted for generating polynomial f(x). The hash value generation part 1211 passes the above hash value Vhsa(s) to the license information assembly part 1212.

[0056]The license information assembly part 1212 passes the decode key Management Department 122 the received issue requesting Dira. The decode key Management Department 122 (refer to drawing 2) manages decode key DB112 (refer to drawing 6 (b)) mentioned above. The decode key Management Department 122

takes out content identifier Icnt and the instrument identification child Idva who are set as the received issue requesting Dira. The decode key Management Department 122 takes out the same decode key Kd as content identifier Icnt to construct from decode key DB112and hands the decode key encryption section 123 together with the instrument identification child Idva. It enciphers using the instrument identification child Idva who received the received decode key Kd simultaneously (Step S29)and the decode key encryption section 123 generates the decode key [finishing / a code] Keda. The above code finishing decode key Keda and the instrument identification child Idva are passed to the license information assembly part 1212.

[0057]The license information assembly part 1212 will start generation of license information Dlca shown in drawing 14 (b)if all the issue requesting Dira and utilization-permission-information Dlwahash value Vhsaand code finishing decode keys Keda are assembled (drawing 12; Step S210). From the issue requesting Dirathe license information assembly part 1212 takes out content identifier Icnt and the instrument identification child Idvaandmore specificallyadds each to the combination of the utilization permission information Dlwathe code finishing decode key Kedaand hash value Vhsa. The license information assembly part 1212 adds the license information identifier Ilc held beforehand to the instrument identification child Idvaand generates license information Dlca. License information Dlca of a more than is the information for controlling the use in the apparatus 21a of the decoding object contents data Decnt. The license information identifier Ilc is information for the apparatus 21a to specify license information Dlca. License information Dlca [more than] is transmitted to the apparatus 21a through the communications department 115 and the transmission line 31 (Step S211).

[0058]In the apparatus 21a (refer to drawing 4)the communications department 213 receives license information Dlca transmitted through the transmission line 31 (Step S212). More specificallythe communications department 213 recognizes having judged that information addressed to itself arrived from the instrument identification child Idva contained in receipt informationand having received license information Dlca from the license information identifier Ilc further set as it this time. According to such a recognition resultthe communications department 213 hands received license information Dlca to the license information treating part 217.

[0059]The license information treating part 217 contains the alteration judgment part 2171the hash value generation part 2172the utilization permission judgment part 2173and the decode key decoding part 2174as shown in drawing 5. License information Dlca from the communications department 213 is first passed to the alteration judgment part 2171. Firstfrom received license information Dlcathe alteration judgment part 2171 takes out the utilization permission information Dlwa and hash value Vhsa (Step S213)passes the taken-out utilization permission information Dlwa to the hash value generation part 2172and holds hash value Vhsa as it is. Herehash value Vhsa taken out at Step S213 is called external hash value Vehsa

from a viewpoint of being generated in the exterior (that isright-of-use controlling device 11) of the apparatus 21a so that confusion may not arise in the following explanation.

[0060]The hash value generation part 2172 holds the same hash function f(x) as the hash value generation part 1211 (refer to drawing 3) by the side of the right-of-use controlling device 11substitutes the received utilization permission information Dlwa for hash function f(x)and generates hash value Vhsa (Step S214). Hash value Vhsa generated at Step S214 here is called internal hash value Vlhsa from a viewpoint of being generated inside the apparatus 21a. The hash value generation part 2172 returns internal hash value Vlhsa [more than] to the alteration judgment part 2171.

[0061]The alteration judgment part 2171 will judge whether the utilization permission information Dlwa is alteredif above-mentioned internal hash value Vlhsa is received (Step S215). Above-mentioned internal hash value Vlhsa(s) are the conditions that the utilization permission information Dlwa in license information Dlca is not alteredandmore specificallyare in agreement with external hash value Vehsa. Thenin Step S215the alteration judgment part 2171 judges whether received internal hash value Vlhsa is in agreement with external hash value Vehsa. When it judges with "Yes"the utilization permission information Dlwa is not alteredbut the alteration judgment part 2171 considers that the utilization permission information Dlwa transmitted this time is effectiveand passes license information Dlca received this time to the utilization permission judgment part 2173.

[0062]The utilization permission judgment part 2173 judges whether use of the decoding object contents data Decnt is permitted with reference to received license information Dlca (Step S216). The utilization permission judgment part 2173 takes out the code finishing decode key Keda from license information Dlca which was restricted when it was judged as "Yes" in Step S216and was receivedand passes it to the decode key decoding part 2174.

[0063]Herean example of processing of the above step S216 is explained. If the above-mentioned assumption is followedreproduction of the contents data Dcnt is permitted only n times by the utilization permission information Dlwa of this license information Dlca. In [this case] Step S216 the utilization permission judgment part 2173If reproduction frequency set as the utilization permission information Dlwa is one or moreit will judge that use of the decoding object contents data Decnt is permittedand received license information Dlca will be passed to the decode key decoding part 2174.

[0064]Although explained in the above example that the right-of-use information Drgt was the reproduction frequency of the contents data Dcntvarious right-of-use information Drgt (that isutilization condition Ccnt) can be set up with this license information managerial system Sa to have mentioned above. Thereforeprocessing of Step S216 needs to be appropriately specified according to the right-of-use information Drgt.

[0065]The decode key decoding part 2174 receives the code finishing decode key Keda from the utilization permission judgment part 2173. The decode key decoding part 2174 takes out the instrument identification child Idva from the instrument identification child storage 211. Thenthe decode key decoding part 2174 decodes the code finishing decode key Keda by the instrument identification child Idva (Step S217)and passes the decode key Kd to the contents decoding part 218.
[0066]By the waythe contents managing department 214 takes out (an example just behind Step S217 is shown in drawing 12)and this decoding object contents data Decnt from the contents accumulating part 215 before the next of the above step S217or it (Step S218). The taken-out decoding object contents data Decnt is passed to the contents decoding part 218. The contents decoding part 218 is the decode key Kd received from the decode key decoding part 2174decodes the decoding object contents data Decnt (Step S219)and passes the contents data Dcnt to the contents reproduction part 219. The contents reproduction part 219 reproduces and carries out voice response of the received contents data Dcnt (Step S220). Therebythe contractor beta can listen to music which the contents data Dcnt purchased from the entrepreneur alpha expresses.
[0067]HereStep S215 of drawing 12 is referred to. In Step S215the alteration judgment part 2171 may judge with the utilization permission information Dlwa being altered. In Step S216the utilization permission judgment part 2173 may judge with use of the decoding object contents data Decnt not being permitted. In such a casethe alteration judgment part 2171 and the utilization permission judgment part 2173 cancel license information Dlca received this time (drawing 13; Step S221). As mentioned abovewith this license information managerial system Saonly when effective license information Dlca is receiveddecoding of the decoding object contents data Decnt is permittedso that clearly. Above-mentioned digital rights are protected by this.
[0068]In Step S24 of drawing 11the right-of-use Management Department 117 may judge that the right-of-use record Rrgt is not registered into right-of-use DB114 (refer to drawing 7 (b)). In Step S25the right-of-use Management Department 117 may judge that a utilization permission cannot be given to the apparatus 21a. In such a casethe right-of-use Management Department 117 generates the use refusal information Drj (refer to drawing 14 (c)) which shows refusing use of the decoding object contents data Decntand hands the communications department 115. The communications department 115 transmits the received use refusal information Drj to the apparatus 21a via the transmission line 31 (drawing 13; Step S222).
[0069]In the apparatus 21a (refer to drawing 4)the communications department 213 receives the use refusal information Drj transmitted through the transmission line 31 (Step S223). By the apparatus 21aprocessing of what is not performed after reception of the use refusal information Drjeither. As mentioned abovewith this license information managerial system Sawhen the right-of-use record Rrgt effective in

right-of-use DB114 is not registeredthe use refusal information Drj is transmitted to the apparatus 21a which becomes transmitting origin of the issue requesting Diraso that clearly. The decoding object contents data Decnt is not decoded in the apparatus 21a side by this. Above-mentioned digital rights are protected by this.
[0070]After the right-of-use Management Department 117 judges that the right-of-use record Rrgt is not registered into right-of-use DB114 (refer to drawing 7 (b))it newly generates the right-of-use record Rrgtand may be made to register with right-of-use DB114 in Step S24.
[0071]Nextregistration of the above right-of-use record Rrgt explains the data communications between the apparatus 21b which is sharing the right of use of the contents data Dcnt with the apparatus 21aand the right-of-use controlling device 11and each operation relevant to it. In operation and almost all the portions of the above-mentioned apparatus 21asince operation of the following apparatus 21b is the sameit simplifies the explanation of operation. Firstthe user beta operates the apparatus 21b and specifies content identifier Icnt and the utilization condition Ccnt. Answering this specificationthe apparatus 21b generates the setting request Drrband transmits to the right-of-use controlling device 11 (drawing 8; Step S11). Since the setting request Drrb is only different at a point including the instrument identification child Idvb who specifies the apparatus 21b as a meaning instead of the instrument identification child Idva as compared with the setting request Drrait omits the detailed explanation. The apparatus 21b may generate the setting request Drrb which does not include the utilization condition Ccntwhen it turns out beforehand that the right-of-use record Rrgt with available self is registered into right-of-use DB114.
[0072]In the right-of-use controlling device 11 (refer to drawing 2)the user authentication part 116 receives the setting request Drrb from the apparatus 21b through the communications department 115. Thenthe user authentication part 116 performs user authentication processing for judging whether the apparatus 21b is a thing of contract user beta (Step S12). The user authentication part 116 passes the right-of-use Management Department 117 the setting request Drrb which was restricted when user authentication processing was successfuland was received.
[0073]The right-of-use Management Department 117 will perform Step S13if it recognizes that this receipt information is the setting request Drrb. In Step S13the right-of-use Management Department 117 first judges whether the right-of-use record Rrgt containing the instrument identification child Idvb and content identifier Icnt in the reception setting demand Drrb is registered into right-of-use DB114 (refer to drawing 7 (b)) (Step S131). As mentioned abovethe right-of-use record Rrgt which originates in the setting request Drra of the apparatus 21aand contains the instrument identification child Idvb and content identifier Icnt in right-of-use DB114 is registered. In this casethe right-of-use Management Department 117 hands this setting request Drrb to the contents managing department 118without performing Steps S132-S133.

[0074]The contents managing department 118 reads the contents data Dcnt and the encryption key Ke after reception of the setting request Drrb (Step S14)and passes them to the contents encryption section 119. The contents managing department 118 passes the reception setting demand Drrb to the send data generation part 120. The contents encryption section 119 passes the code finishing contents data Decnt and the reception setting demand Drrb to the send data generation part 120after performing cipher processing of the contents data Dcnt (Step S15) and completing it.
[0075]As the send data generation part 120 was mentioned aboveit generates send data Dtrnb (refer to drawing 9 (b)) (Step S16). Since send data Dtrnb is only different instead of the instrument identification child Idva at a point including the instrument identification child Idvb as compared with send data Dtrnait omits the detailed explanation. Next it is Step S16the send data generation part 120 passes the communications department 115 send data Dtrnband the communications department 115 transmits received send data Dtrnb to the apparatus 21bas mentioned above (Step S17).
[0076]In the apparatus 21b (refer to drawing 4)the communications department 213 receives send data Dtrnb (Step S18)and hands received-data Dtrnb after that to the contents managing department 214. The contents managing department 214 stores content identifier Icnt in received-data Dtrnband the code finishing contents data Decnt in the contents accumulating part 215 (Step S19).
[0077]From a viewpoint of protection of digital rightslike a case of the apparatus 21aif the apparatus 21b does not receive issue of license information Dlcb from the right-of-use controlling device 11the contents data Dcnt cannot be used for it. Hereafterdrawing 11 - drawing 13 are referred toand operation of the apparatus 21b at the time of acquisition of license information Dlcb and decoding of the contents data Dcnt and the right-of-use controlling device 11 is explained. In operation and almost all portions of the apparatus 21a and the right-of-use controlling device 11since operation at this time is the sameit simplifies that explanation of operation.
[0078]Firstthe user beta operates the apparatus 21b and specifies the decoding object contents data Decnt out of the contents accumulating part 215. Answering the user's beta specificationin the apparatus 21bthe issue requesting generation part 216 generates the issue requesting Dirb (refer to drawing 14 (a))and transmits to the right-of-use controlling device 11 (drawing 11; Step S21). Since the issue requesting Dirb is only different at a point which the instrument identification child Idva replaces with the instrument identification child Idvb as compared with the issue requesting Dirait omits the detailed explanation. The issue requesting generation part 216 passes the communications department 213 the above issue requesting Dirb. The communications department 213 transmits the receiving issue requesting Dirb to the right-of-use controlling device 11.
[0079]In the right-of-use controlling device 11the user authentication part 116 (refer to drawing 2) receives the issue requesting Dirb which the apparatus 21b transmitted

through the communications department 115and performs user authentication processing after that (Step S22). The user authentication part 116 is restricted when user authentication processing is successfuland it passes the right-of-use Management Department 117 the receiving issue requesting Dirb. The right-of-use Management Department 117 takes out the instrument identification child Idvb and content identifier Icnt from the receiving issue requesting Dirb (Step S23)Thenit is judged whether the right-of-use record Rrgt containing the instrument identification child Idvb who took outand the same thing as combination of content identifier Icnt is registered into right-of-use DB114 (refer to drawing 7 (b)) (Step S24).

[0080]The right-of-use Management Department 117 refers to the right-of-use information Drgt included in the target right-of-use record Rrgtwhen it is judged as "Yes" at Step S24It is judged whether the right of use of whether a utilization permission can be given to the apparatus 21b and the contents data Dcnt that isremains (Step S25). When it is judged as "Yes" at Step S25the right-of-use Management Department 117 generates the utilization permission information Dlwb using the target right-of-use information Drgt (Step S26). Since the utilization permission information Dlwb is different only at the point which the instrument identification child Idva replaces with the instrument identification child Idvb as compared with the utilization permission information Dlwait omits the detailed explanation. It is Step S26next only the part for which the right-of-use Management Department 117 was used at Step S26 updates the right-of-use information Drgt (Step S27).

[0081]The right-of-use Management Department 117 (refer to drawing 2) hands the above utilization permission information Dlwb to the license information generation part 121 together with the issue requesting Dirb. In the license information generation part 121the hash value generation part 1211 (refer to drawing 3)The received utilization permission information Dlwb is substituted for hash function f(x) held beforehandhash value Vhsb for carrying out which prevents the alteration of the utilization permission information Dlwb is generated to it (Step S28)and it is passed to it at the license information assembly part 1212.

[0082]The license information assembly part 1212 passes the decode key Management Department 122 the received issue requesting Dirb. The decode key Management Department 122 (refer to drawing 2) has managed decode key DB112 (refer to drawing 6 (b)) mentioned aboveand takes out content identifier Icnt and the instrument identification child Idvb from the receiving issue requesting Dirb. The decode key Management Department 122 takes out the same decode key Kd as content identifier Icnt to construct from decode key DB112and hands the decode key encryption section 123 together with the instrument identification child Idvb. It enciphers using the instrument identification child Idvb who received the received decode key Kd simultaneously (Step S29)and the decode key encryption section 123 generates the code finishing decode key Kedb. The above code finishing decode key

Kedb and the instrument identification child Idvb are passed to the license information assembly part 1212.
[0083]The license information assembly part 1212 will generate license information Dlcb (refer to drawing 14 (b))if all the issue requesting Dirb and utilization-permission-information Dlwbhash value Vhsband code finishing decode keys Kedb are assembled (drawing 12; Step S210). As compared with license information Dlcalicense information Dlcb. Since it is only different at the point which the instrument identification child Idvathe utilization permission information Dlwathe code finishing decode key Kedaand hash value Vhsa replace with the instrument identification child Idvbthe utilization permission information Dlwbthe code finishing decode key Kedband hash value Vhsbthe detailed explanation is omitted. License information Dlcb of a more than is transmitted to the apparatus 21b through the communications department 115 and the transmission line 31 (Step S211).
[0084]In the apparatus 21b (refer to drawing 4)the communications department 213 receives license information Dlcb transmitted through the transmission line 31 (Step S212)and hands it to the license information treating part 217. In the license information treating part 217the alteration judgment part 2171From receiving license information Dlcbthe utilization permission information Dlwb and hash value Vhsb are taken out (Step S213)the taken-out utilization permission information Dlwb is passed to the hash value generation part 2172and hash value Vhsb is held as external hash value Vehsb. The hash value generation part 2172 holds the same hash function f(x) as the right-of-use controlling device 11 sidesubstitutes the received utilization permission information Dlwb for hash function f(x)generates internal hash value Vlhsb (Step S214)and returns it to the alteration judgment part 2171.
[0085]Like the above-mentionedif above-mentioned internal hash value Vlhsb is receivedthe alteration judgment part 2171Receiving license information Dlcb is passed to the utilization permission judgment part 2173 noting that this utilization permission information Dlwb is effectivewhen it judges whether it is in agreement with external hash value Vehsb (Step S215) and both are in agreement. The utilization permission judgment part 2173 judges whether use of the decoding object contents data Decnt is permitted like the above-mentioned (Step S216)The code finishing decode key Kedb is taken out from license information Dlcb which was restricted when it was judged as "Yes"and was receivedand the decode key decoding part 2174 is passed. The decode key decoding part 2174 receives the code finishing decode key Kedb from the utilization permission judgment part 2173. The decode key decoding part 2174 takes out the instrument identification child Idvb from the instrument identification child storage 211. Thenthe decode key decoding part 2174 decodes the code finishing decode key Kedb by the instrument identification child Idvb (Step S217)and passes the decode key Kd obtained as a result to the contents decoding part 218.
[0086]The contents managing department 214 takes out this decoding object contents data Decnt from the contents accumulating part 215 (Step S218)and passes

it to the contents decoding part 218. The contents decoding part 218 is the decode key Kd from the decode key decoding part 2174decodes the decoding object contents data Decnt (Step S219)and passes the contents data Dcnt to the contents reproduction part 219. The contents reproduction part 219 reproduces and carries out voice response of the received contents data Dcnt (Step S220).

[0087]According to this embodimenttwo or more instrument identification children Idva and Idvb are recorded on the right-of-use record Rrgt as mentioned above. Even if the issue requesting Dira and Dirb has been transmitted from the apparatus 21a and 21b from which the right-of-use controlling device 11 differs mutually by thisit is referring to the right-of-use record RrgtThey can be provided now with license information Dlca and Dlcb which were generated from the same right-of-use information Drgt. By this above embodimentright management technology in which digital rights with two or more common apparatus are sharable can be provided.

[0088]In an above embodimentalthough the right-of-use record Rrgt contained the group identification descriptor Igpthis is for clarifying that the apparatus 21a and 21b belongs to the same group. That isthe group identification descriptor Igp is not information indispensable on the right-of-use record Rrgt. It may be made for the right-of-use record Rrgt to specify the apparatus 21a and 21b belonging to the same group only using the group identification descriptor Igpwithout including the instrument identification children Idva and Idvb of the apparatus 21a and 21b.

[0089]Although two sets of the apparatus 21a and the apparatus 21b were mentioned as an example of representation of two or more apparatus 21it may be made for an above embodiment to share the same right-of-use information Drgt not only by this but by three sets or more of apparatus.

[0090]In an above embodimenton account of a graphic displayalthough it explained that the right-of-use controlling device 11 was provided with contents DB111not only this but the contents data Dcnt may be distributed to the apparatus 21a and 21b from another server.

[0091]By an above embodimentthe apparatus 21a and 21b registered into User Information DB113 at the time of a contract explained an example which shares the same right-of-use information Drgt. Howeverthe users' beta apparatus 21 does not necessarily receive contents distribution only by two sets of the apparatus 21a and 21band there is to use the contents data Dcnt using the apparatus 21 which came to hand newly. Right-of-use controlling device 11a -11d explained below is the 1st of the above-mentioned right-of-use controlling device 11 - the 4th modificationand it is provided in order to satisfy above-mentioned needs. "The 1st modification"

[0092]Drawing 15 is a block diagram showing an entire configuration of license information managerial system Sa1 which accommodated the right-of-use controlling device 11a. License information managerial system Sa1 of drawing 15 is different at a point which replaced with the right-of-use controlling device 11 as compared with the license information managerial system Sa of drawing 1and is provided with the right-

of-use controlling device 11aand a point further provided with the apparatus 21c. Since there is no point of difference in both the license information managerial systems Sa and Sa1 in addition to itin drawing 15the same reference mark is attached to a thing equivalent to composition of drawing 1and each explanation is omitted. Although the telecommunication cable 32 is shown in drawing 15since this is composition used by the 4th modificationit omits explanation of the telecommunication cable 32 not only by this modification but by the 2nd and 3rd modifications.

[0093]The right-of-use controlling device 11a is installed in the above-mentioned entrepreneur alpha sideand as shown in drawing 16 as compared with the right-of-use controlling device 11 of drawing 2it is different at the point further provided with the User Information Management Department 124 and the registration completion generation part 125. There is no point of difference among both the rights-of-use controlling devices 11 and 11a in addition to it. Soin drawing 16a graphic display and explanation of composition of that there is no relation among the things equivalent to the composition of drawing 2 in this modification are omitted.

[0094]Although the apparatus 21c is owned by the above-mentioned user betaAt presentit is apparatus unregistered to User Information DB113 of the right-of-use controlling device 11aand as shown in drawing 17 as compared with the apparatus 21a or 21b of drawing 4it is different at the point further provided with the registry request generation part 220 and the group identification descriptor storage 221. In addition to itthere is no point of difference between both the apparatus 21a and 21b and the apparatus 21c. Soin drawing 17a graphic display and explanation of composition of that there is no relation among the things equivalent to the composition of drawing 4 in this modification are omitted. The instrument identification child Idvc for specifying the apparatus 21c as a meaning is beforehand stored in the instrument identification child storage 211 of the apparatus 21cand it is assumed that the group identification descriptor Igp assigned to the user beta is stored in the group information storage 221.

[0095]Nextwith reference to drawing 18operation of the apparatus 21c until it registers the apparatus 21c into User Information DB113and the right-of-use controlling device 11a is explained in license information managerial system Sa1 of the above composition. Firstthe apparatus 21c stores in the group identification descriptor storage 221 the group identification descriptor Igp to which the user beta is notified by the entrepreneur alpha according to the user's beta operation. Thenthe user beta operates the apparatus 21c and specifies registering this apparatus 21c into User Information DB113. Answering this specificationin the apparatus 21cthe registry request generation part 220 generates the registry request Drsc shown in drawing 19 (a)and transmits to the right-of-use controlling device 11a (drawing 18; Step S31). The registry request Drsc is the information for requiring this apparatus 21c of the right-of-use controlling device 11a as registering with User Information

DB113. When Step S31 is explained more concretelyfirst the registry request generation part 220Take out the instrument identification child Idvc from the instrument identification child storage 211and furtherAfter taking out the group identification descriptor Igp from the group identification descriptor storage 221the registry request identifier Irs held beforehand is added to combination of the taken-out group identification descriptor Igp and the instrument identification child Idvcand the registry request Drsc (refer to drawing 19 (a)) is generated. Heresince the right-of-use controlling device 11a specifies the registry request Drscthe registry request identifier Irs is used. The registry request generation part 220 passes the communications department 213 the above registry request Drsc. The communications department 213 transmits the received registry request Drsc to the right-of-use controlling device 11a through the transmission line 31.

[0096]In the right-of-use controlling device 11a (refer to drawing 16)the communications department 115 receives information transmitted through the transmission line 31and recognizes that this receipt information is the registry request Drsc from the registry request identifier Irs contained in it. According to this recognition resultthe communications department 115 hands the User Information Management Department 124 the receiving registry request Drsc. The User Information Management Department 124 searches the contractor record Rcs (refer to drawing 7 (a)) containing the group identification descriptor Igp which accessed User Information DB113 and was taken outafter taking out the group identification descriptor Igp from the receiving registry request Drsc (Step S32). The User Information Management Department 124 takes out the number Ndv of instrument identification children from the searched contractor record Rcs (Step S33).

[0097]Nextthe User Information Management Department 124 judges whether it is more than the upper limit Vul as which the taken-out number Ndv of instrument identification children was determined beforehand (Step S34). Herethe user beta of the upper limit Vul is the upper limit of the number of apparatus which can be registered into User Information DB113. When it is judged that it is Step S34 and the number Ndv of instrument identification children is not more than the upper limit Vulthe User Information Management Department 124 takes out the instrument identification child Idvc from the receiving registry request Drscand adds what was taken out to the target contractor record Rcs (Step S35). The User Information Management Department 124 **********s the number Ndv of instrument identification children only 1 (Step S36). As a resultthe contractor record Rcs is updated by the thing as shown in drawing 20 from what is shown in drawing 7 (a). Thenthe User Information Management Department 124 notifies the registration completion generation part 125 that the contractor record Rcs was updated correctlyand hands the instrument identification child Idvc in the receiving registry request Drsc further to the registration completion generation part 125.

[0098]If it is reported that renewal of the contractor record Drsc was completed from

the User Information Management Department 124the registration completion generation part 125 will generate the notice Dscc of registration completion shown in drawing 19 (b)and will transmit to the apparatus 21c (Step S37). The notice Dscc of registration completion is the information for notifying the apparatus 21c that this apparatus 21c was correctly registered into User Information DB113. If Step S37 is explained more concretelyfirstthe registration completion generation part 125 will add the registration completion identifier Isc held beforehand to the instrument identification child Idvc who received from the User Information Management Department 124and will generate the notice Dscc of registration completion (refer to drawing 19 (b)). Heresince the apparatus 21c specifies the notice Dscc of registration completionthe registration completion identifier Isc is used. The registration completion generation part 125 passes the communications department 115 the above notice Dscc of registration completion. The communications department 115 transmits the received notice Dscc of registration completion to the apparatus 21c through the transmission line 31.

[0099]In the apparatus 21c (refer to drawing 17)the communications department 213 receives information transmitted through the transmission line 31and recognizes that this receipt information is the notice Dscc of registration completion from the registration completion identifier Isc contained in it. According to this recognition resultthe communications department 213 hands the notice Dscc of receiving registration completion to the setting request generation part 212. The setting request generation part 212 recognizes having received the notice Dscc of registration completion this time from the registration completion identifier Isc set as receipt information (Step S38). It judges that the setting request generation part 212 changed into a state where Step S11 of drawing 8 can be performedaccording to this recognition resultand the right-of-use controlling device 11a and data communications are performed henceforth like the apparatus 21a or the apparatus 21b explained by a 1st embodiment.

[0100]Since the data communications of the right-of-use controlling device 11a and the apparatus 21c enable the user beta to register the instrument identification child Idvc of the new apparatus 21c which came to hand into User Information DB113 as mentioned above according to this modificationMore user-friendly license information managerial system Sa1 can be provided now.

[0101]When the number Ndv of instrument identification children is judged to be more than the upper limit Vul in Step S34the User Information Management Department 124It notifies the registration completion generation part 125 that renewal of the contractor record Rcs is refusedwithout performing processing like Steps S35-S36and the instrument identification child Idvc in the receiving registry request Drsc is further passed to the registration completion generation part 125. If updating refusal of the contractor record Drsc is notifiedthe registration completion generation part 125 will generate the notice Dsrc of a register reject shown in drawing 19 (c)and

will transmit to the apparatus 21c through the communications department 213 and the transmission line 31 (Step S39). The notice Drsc of a register reject is the information for notifying the apparatus 21c that this apparatus 21c cannot be registered into User Information DB113and contains the register-reject identifier Isr beforehand held with the instrument identification child Idvc who received from the User Information Management Department 124. In the apparatus 21c (refer to drawing 17)the setting request generation part 212 receives the notice Dsrc of a register reject through the communications department 213 (Step S310)judges that the setting request generation part 212 is not in the state where Step S11 of drawing 8 can be performed according to the noticeand ends processing.

[0102]In Step S32the User Information Management Department 124When the contractor record Rcs (refer to drawing 7 (a)) containing the taken-out group identification descriptor Igp cannot be foundit is preferred to perform the same processing as Step S39and to refuse registration to User Information DB113 of the instrument identification child Idvc.

[0103]In the above modification [1st]when the apparatus 21c and the right-of-use controlling device 11a performed data communicationsthe instrument identification child Idvc was registered into User Information DB113. Howevernot only like this but like the following the 2nd - 4th modificationthe apparatus 21cand other apparatus 21a or apparatus 21b collaborateand the instrument identification child Idvc may be made to be registered into User Information DB113.

[0104]An entire configuration of license information managerial system Sa2 which accommodated the right-of-use controlling device 11b concerning the "2nd modification"next the 2nd modification is explained. License information managerial system Sa2 is different at a point which replaced with the right-of-use controlling device 11and is provided with the right-of-use controlling device 11band a point further provided with the apparatus 21cas shown in drawing 15 as compared with the license information managerial system Sa of drawing 1. Since there is no point of difference in both the license information managerial systems Sa and Sa2 in addition to itin drawing 15the same reference mark is attached to a thing equivalent to composition of drawing 1and each explanation is omitted.

[0105]The right-of-use controlling device 11b is installed in the above-mentioned entrepreneur alpha sideand as shown in drawing 21 as compared with the right-of-use controlling device 11 of drawing 2it is different at a point further provided with the User Information Management Department 126 and the registration completion generation part 127. There is no point of difference among both the rights-of-use controlling devices 11 and 11b in addition to it. Soin drawing 21a graphic display and explanation of composition of that there is no relation among things equivalent to composition of drawing 2 in this modification are omitted.

[0106]As a 1st embodiment explained the apparatus 21a or the apparatus 21bit is owned by the user beta and each instrument identification child Idva and Idvb is still

more nearly registered to User Information DB113 of the right-of-use controlling device 11b (refer to drawing 7 (a)). The apparatus 21a or 21b is different at a point further provided with the instrument identification child input part 222the provisional registration demand generation part 223and the completion outputting part 224 of provisional registrationas shown in drawing 22 as compared with drawing 4 for registration of the instrument identification child Idvc of the apparatus 21c. There is no point of difference between the apparatus 21a and 21b applied to this modification in addition to itand a thing concerning a 1st embodiment. Soin drawing 22a graphic display and explanation of composition unrelated to this modification among things equivalent to composition of drawing 4 are omitted.

[0107]Although the apparatus 21c is owned by the above-mentioned user betaAt presentit is apparatus unregistered to User Information DB113 of the right-of-use controlling device 11band as shown in drawing 23 as compared with the apparatus 21a or 21b of drawing 4it is different at the point further provided with the instrument identification child input part 225 and the high-grade-registry demand generation part 226. In addition to itthere is no point of difference between both the apparatus 21a and 21b and the apparatus 21c. Soin drawing 23a graphic display and explanation of composition unrelated to this modification among the things equivalent to the composition of drawing 4 are omitted.

[0108]Nextwith reference to drawing 24 and drawing 25operation of the apparatus 21a until it registers the instrument identification child Idvc of the apparatus 21c into User Information DB113the apparatus 21cand the right-of-use controlling device 11b is explained in license information managerial system Sa2 of the above composition. The user beta operates the apparatus 21a and specifies registering the instrument identification child Idvc provisionally into User Information DB113. In relation to this specificationthe instrument identification child input part 222 of the apparatus 21a notifies the instrument identification child Idvc of the apparatus 21c inputted when the user beta operated the apparatus 21a to the provisional registration demand generation part 223 (drawing 24; Step S41). Herein the following explanationthe instrument identification child Idvc of the apparatus 21c is called the registering object identifier Idvc. The provisional registration demand generation part 223 answers an above-mentioned noticegenerates the provisional registration demand Dprsc shown in drawing 26 (a)and transmits to the right-of-use controlling device 11b (Step S42). The provisional registration demand Dprsc is the information for requiring the registering object identifier Idvc of the right-of-use controlling device 11b as registering provisionally with User Information DB113. If Step S42 is explained concretelythe provisional registration demand generation part 223 will treat the instrument identification child Idva who took out as the registered identifier Idva firstafter taking out the instrument identification child Idva from the instrument identification child storage 211. And the provisional registration demand generation part 223 adds the provisional registration demand identifier Iprs held beforehand to

combination of the registered identifier Idva and the registering object identifier Idvcand generates the provisional registration demand Dprsc (refer to drawing 26 (a)). Heresince the right-of-use controlling device 11b specifies the provisional registration demand Dprscthe provisional registration demand identifier Iprs is used. The provisional registration demand generation part 223 passes the communications department 213 the above provisional registration demand Dprsc. The communications department 213 transmits the received provisional registration demand Dprsc to the right-of-use controlling device 11b through the transmission line 31.

[0109]In the right-of-use controlling device 11b (refer to drawing 21)since the provisional registration demand identifier Iprs is contained in receipt information from the transmission line 31the communications department 115 recognizes having received the provisional registration demand Dprsc this time. According to this recognition resultthe communications department 115 hands the User Information Management Department 126 the reception provisional registration demand Dprsc. The User Information Management Department 126 searches the contractor record Rcs (refer to drawing 7 (a)) containing the registered identifier Idva which accessed User Information DB113 and was taken outafter taking out the registered identifier Idva from the reception provisional registration demand Dprsc (Step S43). Thenin [the User Information Management Department 126 performs the same processing as Steps S33 and S34 of drawing 18 (Step S44S45)and] Step S45When it is judged that the number Ndv of instrument identification children is not less than the upper limit Vulthe same processing as Step S39 of drawing 18 is performed (Step S46). In this casethe apparatus 21a performs the same processing as Step S310 of drawing 18 (Step S47).

[0110]What was taken out after taking out the registering object identifier Idvc from the reception provisional registration demand Dprscwhen it is judged in Step S45 to it that the number Ndv of instrument identification children is less than the upper limit VulThe provisional registration flag Fps which shows that he is the instrument identification child Idvc by whom it was registered provisionally is added to the target contractor record Rcs (Step S48). The contractor record Rcs is updated by the thing as shown in drawing 27 (a) from what is shown in drawing 7 (a). Thenthe User Information Management Department 126 notifies the registration completion generation part 127 that provisional registration of the registering object identifier Idvc was completedand hands the registered identifier Idva in the reception provisional registration demand Dprsc further to the registration completion generation part 127.

[0111]If it is reported that provisional registration was completed from the User Information Management Department 126the registration completion generation part 127 will generate the provisional registration completion notification Dpscc shown in drawing 26 (b)and will transmit to the apparatus 21a (Step S49). The provisional

registration completion notification Dpscc is the information for notifying the apparatus 21a that the registering object identifier Idvc was registered provisionally into User Information DB113. If Step S48 is explained more concretelyfirstthe registration completion generation part 127 will add the completion identifier Ipsc of provisional registration held beforehand to the registered identifier Idva received from the User Information Management Department 126and will generate the provisional registration completion notification Dpscc (refer to drawing 26 (b)). Heresince the apparatus 21a specifies the provisional registration completion notification Dpsccthe completion identifier Ipsc of provisional registration is used. The above provisional registration completion notification Dpscc is transmitted to the apparatus 21a through the communications department 115 and the transmission line 31 from the registration completion generation part 127.

[0112]In the apparatus 21a (refer to drawing 22)the communications department 213 recognizes that this receipt information is the provisional registration completion notification Dpscc addressed to itself from the completion identifier Ipsc of provisional registration contained in the receipt information from the transmission line 31and the registered identifier Idva. According to this recognition resultthe communications department 213 hands the reception provisional registration completion notification Dpscc to the completion outputting part 224 of provisional registration. The completion outputting part 224 of provisional registration answers the completion Dpscc of reception provisional registrationoutputs that the instrument identification child's Idvc provisional registration was completed with a picture or a sound (Step S410)and tells that to the user beta. By thisthe processing by the side of the apparatus 21a is completed.

[0113]If the completion of provisional registration is recognizedthe user beta will operate the apparatus 21c and will specify carrying out high grade registry of the instrument identification child Idvc to User Information DB113. In relation to this specificationthe instrument identification child input part 225 of the apparatus 21c notifies the instrument identification child (registered identifier) Idva of the apparatus 21a inputted when the user beta operated the apparatus 21c to the high-grade-registry demand generation part 226 (drawing 25; Step S51). Answering this noticethe high-grade-registry demand generation part 226 generates the high-grade-registry demand Dcrsc shown in drawing 28 (a)and transmits to the right-of-use controlling device 11b (Step S52). The high-grade-registry demand Dcrsc is the information for requiring the instrument identification child Idvc of the right-of-use controlling device 11b as carrying out high grade registry to User Information DB113. When Step S52 is explained concretelyfirst the high-grade-registry demand generation part 226The registering object identifier Idvc taken out after taking out the instrument identification child (getting it blocked registering object identifier) Idvc from the instrument identification child storage 211. The high-grade-registry demand identifier Icrs held beforehand is added to combination with the notified registered identifier

Idvaand the high-grade-registry demand Dcrsc (refer to drawing 28 (a)) is generated. Heresince the right-of-use controlling device 11b specifies the high-grade-registry demand Dcrscthe high-grade-registry demand identifier Icrs is used. The high-grade-registry demand generation part 226 transmits the above high-grade-registry demand Dcrsc to the right-of-use controlling device 11b through the communications department 213 and the transmission line 31.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the entire configuration of the license information managerial system Sa which accommodated the right-of-use controlling device 11 concerning a 1st embodiment of this invention.

[Drawing 2]It is a block diagram showing the detailed composition of the right-of-use controlling device 11 of drawing 1.

[Drawing 3]It is a block diagram showing the detailed composition of the license information generation part 121 of drawing 2.

[Drawing 4]It is a block diagram showing the detailed composition of the apparatus 21a and 21b of drawing 1.

[Drawing 5]It is a block diagram showing the detailed composition of the license information treating part 217 of drawing 4.

[Drawing 6]It is a mimetic diagram showing contents DB111 of drawing 2and decode key DB112 of drawing 2.

[Drawing 7]It is a mimetic diagram showing User Information DB113 of drawing 2and right-of-use DB114 of drawing 2.

[Drawing 8]It is a flow chart which shows operation of the apparatus 21a at the time of right-of-use setting out of the contents data Dcntand acquisitionand the right-of-use controlling device 11.

[Drawing 9]It is a mimetic diagram showing the format of the setting request Drr sent and received in process of the processing shown in drawing 8and send data Dtrn.

[Drawing 10]It is a mimetic diagram showing the data stored in the contents accumulating part 215 of drawing 4.

[Drawing 11]It is the 1st flow chart that shows operation of the apparatus 21a at the time of acquisition of license information Dlcaand decoding of the contents data Dcntand the right-of-use controlling device 11.

[Drawing 12]It is the 2nd flow chart that shows operation of the apparatus 21a at the time of acquisition of license information Dlcaand decoding of the contents data Dcntand the right-of-use controlling device 11.

[Drawing 13]It is the 3rd flow chart that shows operation of the apparatus 21a at the time of acquisition of license information Dlcaand decoding of the contents data Dcntand the right-of-use controlling device 11.

[Drawing 14]It is a mimetic diagram showing the format of the issue requesting Dir sent and received in process of processing of drawing 12 – drawing 13the license information Dlcand the use refusal information Drj.
[Drawing 15]It is a block diagram showing the entire configuration of license information managerial system Sa1 which accommodated the right-of-use controlling device 11a concerning the 1st modification of the right-of-use controlling device 11 of drawing 1.
[Drawing 16]It is a block diagram showing the detailed composition of the right-of-use controlling device 11a shown in drawing 15.
[Drawing 17]It is a block diagram showing the detailed composition of the apparatus 21c shown in drawing 15.
[Drawing 18]It is a flow chart which shows operation of the apparatus 21c until it registers the apparatus 21c of drawing 15 into User Information DB113and the right-of-use controlling device 11a.
[Drawing 19]It is a mimetic diagram showing the format of the registry request Drsc and the notice Dscc of registration completion which are sent and received in process of processing of drawing 18and the notice Dsrc of a register reject.
[Drawing 20]It is a mimetic diagram showing User Information DB113 updated by processing of drawing 18.
[Drawing 21]It is a block diagram showing the detailed composition of the right-of-use controlling device 11b concerning the 2nd modification of the right-of-use controlling device 11 of drawing 1.
[Drawing 22]It is a block diagram showing the detailed composition of the apparatus 21a or 21b concerning the 2nd modification.
[Drawing 23]It is a block diagram showing the detailed composition of the apparatus 21c concerning the 2nd modification.
[Drawing 24]It is a flow chart which shows operation of the apparatus 21a at the time of registering the instrument identification child Idvc of the apparatus 21c into User Information DB113and the right-of-use controlling device 11b.
[Drawing 25]It is a flow chart which shows operation of the apparatus 21c at the time of registering the instrument identification child Idvc of the apparatus 21c into User Information DB113and the right-of-use controlling device 11b.
[Drawing 26]It is a mimetic diagram showing the provisional registration demand Dprsc sent and received in process of processing of drawing 24and the format of the provisional registration completion notification Dpscc.
[Drawing 27]It is a mimetic diagram showing User Information DB113 updated by processing of drawing 24 and drawing 25.
[Drawing 28]It is a mimetic diagram showing the high-grade-registry demand Dcrsc sent and received in process of processing of drawing 25and the format of the high-grade-registry completion notification Dcscc.
[Drawing 29]It is a block diagram showing the detailed composition of the right-of-use

controlling device 11c concerning the 3rd modification of the right-of-use controlling device 11 of drawing 1.
[Drawing 30]It is a block diagram showing the detailed composition of the apparatus 21a or 21b concerning the 3rd modification.
[Drawing 31]It is a block diagram showing the detailed composition of the apparatus 21c concerning the 3rd modification.
[Drawing 32]It is a flow chart which shows operation of the apparatus 21c at the time of registering the instrument identification child Idvc of the apparatus 21c into User Information DB113and the right-of-use controlling device 11c.
[Drawing 33]It is a flow chart which shows operation of the apparatus 21a at the time of registering the instrument identification child Idvc of the apparatus 21c into User Information DB113and the right-of-use controlling device 11c.
[Drawing 34]It is a mimetic diagram showing the format of the password demand Drps sent and received in process of processing of drawing 32and password notice Dpss.
[Drawing 35]It is a mimetic diagram showing User Information DB113 updated by processing of drawing 32 and drawing 33.
[Drawing 36]It is a mimetic diagram showing the format of the registry request Drsc and the notice Dscc of registration completion which are sent and received in process of processing of drawing 33.
[Drawing 37]It is a block diagram showing the detailed composition of the right-of-use controlling device 11d concerning the 4th modification of the right-of-use controlling device 11 of drawing 1.
[Drawing 38]It is a block diagram showing the detailed composition of the apparatus 21a or 21b concerning the 4th modification.
[Drawing 39]It is a block diagram showing the detailed composition of the apparatus 21c concerning the 4th modification.
[Drawing 40]It is a flow chart which shows operation of the apparatus 21a until it registers the instrument identification child Idvc of the apparatus 21c into User Information DB113the apparatus 21cand the right-of-use controlling device 11d.
[Drawing 41]It is a figure showing the 1st registry request Drscthe1 sent and received in process of processing of drawing 40and 2nd registry request Drscand the format of the notice Dscc of registration completion.
[Drawing 42]It is a block diagram showing the entire configuration of license information managerial system Sa5 which accommodated the right-of-use controlling device 11e concerning the 5th modification of the right-of-use controlling device 11 of drawing 1.
[Drawing 43]It is a block diagram showing the detailed composition of the right-of-use controlling device 11e shown in drawing 42.
[Drawing 44]It is a block diagram showing the detailed composition of the apparatus 21b shown in drawing 42.
[Drawing 45]It is a flow chart which shows operation of the apparatus 21b until it

deletes the instrument identification child Idvb of the apparatus 21b from User Information DB113 and right-of-use DB114and the right-of-use controlling device 11e.

[Drawing 46]It is a mimetic diagram showing the format of the deletion request Drwb sent and received in process of processing of drawing 45and the deletion completion notice Dswb.

[Drawing 47]It is a mimetic diagram showing User Information DB113 updated by processing of drawing 45.

[Drawing 48]It is a block diagram showing the entire configuration of the license information managerial system Sb which accommodated the right-of-use controlling device 41 concerning a 2nd embodiment of this invention.

[Drawing 49]It is a block diagram showing the detailed composition of the right-of-use controlling device 41 of drawing 48.

[Drawing 50]It is a block diagram showing the detailed composition of the apparatus 51a and 51b of drawing 48.

[Drawing 51]It is a flow chart which shows operation of the apparatus 51a at the time of acquisition of the contents data Dcntand the right-of-use controlling device 41.

[Drawing 52]It is a mimetic diagram showing right-of-use DB114 of drawing 49.

[Drawing 53]It is a figure showing the format of 2nd setting request Drr2b sent and received in process of processing of drawing 51.

[Drawing 54]It is a block diagram showing the entire configuration of license information managerial system Sc concerning a 3rd embodiment of this invention.

[Drawing 55]It is a functional block diagram showing the detailed composition of the right-of-use controlling device 71 of drawing 54.

[Drawing 56]It is a figure showing the detailed composition of the license information generation part 721 of drawing 55.

[Drawing 57]It is a functional block diagram showing the detailed composition of the apparatus 81 of drawing 54.

[Drawing 58]It is a functional block diagram showing the detailed composition of the license information treating part 817 of drawing 57.

[Drawing 59]It is a mimetic diagram showing contents DB711 of drawing 55and decode key DB712 of drawing 55.

[Drawing 60]It is a mimetic diagram showing User Information DB713 and right-of-use DB714 of drawing 55.

[Drawing 61]It is a flow chart which shows operation of the apparatus 81 at the time of acquisition of the contents data Dcntand the right-of-use controlling device 71.

[Drawing 62]It is a mimetic diagram showing the format of the setting request Drr sent and received in process of processing of drawing 61and send data Dtrn.

[Drawing 63]It is a mimetic diagram showing the data stored in the contents accumulating part 815 of drawing 58.

[Drawing 64]It is the 1st flow chart that shows operation of the apparatus 81 at the

time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Drawing 65]It is the 2nd flow chart that shows operation of the apparatus 81 at the time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Drawing 66]It is the 3rd flow chart that shows operation of the apparatus 81 at the time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Drawing 67]It is a mimetic diagram showing the format of the issue requesting Dir sent and received in process of processing of drawing 64 - drawing 66the license information Dlcand the use refusal information Drj.
[Drawing 68]It is a block diagram showing the entire configuration of license information managerial system Sc1 concerning the modification of license information managerial system Sc of drawing 54.
[Drawing 69]It is a mimetic diagram showing the composition of the portability type recording medium 101 of drawing 68.
[Drawing 70]It is a functional block diagram showing the detailed composition of the apparatus 201 of drawing 68.
[Drawing 71]It is a mimetic diagram showing User Information DB713 and right-of-use DB714 of drawing 68.
[Drawing 72]It is the 1st flow chart that shows operation of the apparatus 201 concerned at the time of the contractor beta acquiring the contents data Dcnt using the apparatus 201and the right-of-use controlling device 71.
[Drawing 73]It is the 2nd flow chart that shows operation of the apparatus 201 concerned at the time of the contractor beta acquiring the contents data Dcnt using the apparatus 201and the right-of-use controlling device 71.
[Drawing 74]It is a mimetic diagram showing the format of the setting request Drr and the issue requesting Dir which are sent and received in process of processing of drawing 72 and drawing 73.
[Drawing 75]It is the 1st flow chart that shows operation of the apparatus 201 at the time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Drawing 76]It is the 2nd flow chart that shows operation of the apparatus 201 at the time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Drawing 77]It is the 3rd flow chart that shows operation of the apparatus 201 at the time of acquisition of the license information Dlcand decoding of the contents data Dcntand the right-of-use controlling device 71.
[Explanations of letters or numerals]
SaSa1-Sa5SbScSc1 -- License information managerial system
1111a - 11e4171 -- Right-of-use controlling device

21a -21c51a51b81201 -- Apparatus
101 -- Portability type recording medium

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－173381
（P2003－173381A）
(43)公開日　平成15年６月20日(2003.6.20)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　17/60	１４２	Ｇ０６Ｆ　17/60	１４２	５Ｂ０１７
	３０２		３０２Ｅ	５Ｂ０８５
12/14	３２０	12/14	３２０Ｆ	５Ｊ１０４
15/00	３３０	15/00	３３０Ｂ	
			３３０Ｚ	

審査請求　未請求　請求項の数22　ＯＬ　（全 60 頁）　最終頁に続く

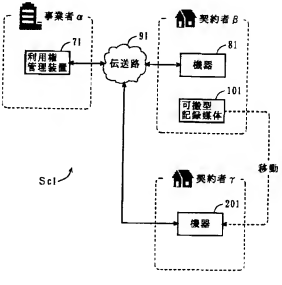
(21)出願番号　特願2002－154341(P2002－154341)
(22)出願日　平成14年５月28日(2002.5.28)
(31)優先権主張番号　特願2001－160290(P2001－160290)
(32)優先日　平成13年５月29日(2001.5.29)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－224413(P2001－224413)
(32)優先日　平成13年７月25日(2001.7.25)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－291593(P2001－291593)
(32)優先日　平成13年９月25日(2001.9.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　大館　雅博
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　上坂　靖
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100098291
弁理士　小笠原　史朗

最終頁に続く

(54)【発明の名称】　利用権管理装置

(57)【要約】
【課題】　他者の機器上で、自分の利用権情報を使って、コンテンツデータを利用可能な利用権管理装置を提供すること
【解決手段】　契約者γの機器２０１は、契約者βの可搬型記録媒体１０１内のメディア識別子を使って、コンテンツデータの利用許可を受けるための発行要求を生成し、利用権管理装置７１に送信する。利用権管理装置７１は、契約者βに与えられたコンテンツデータの利用権情報を管理し、当該利用権情報と、発行要求とを使って、可搬型記録媒体１０１にコンテンツデータの利用を許可する利用許可情報を生成する。さらに、利用権管理装置７１は、利用許可情報に基づいて、可搬型記録媒体１０１に接続された機器におけるコンテンツデータの利用を制御するライセンス情報を生成して、機器２０１に送信する。機器２０１は、ライセンス情報を処理して、コンテンツデータの利用を制御する。



【特許請求の範囲】

【請求項１】　複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、

前記複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権ＤＢと称する）と、

各前記機器からの発行要求に応答して、前記利用権ＤＢに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、

前記利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、

前記ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える、利用権管理装置。

【請求項２】　前記機器は、コンテンツデータの利用条件を少なくとも含む設定要求を送信し、

前記利用権管理部は、前記機器からの設定要求に応答して、少なくとも設定要求を送信した機器に対する利用権情報を前記利用権ＤＢに登録する、請求項１に記載の利用権管理装置。

【請求項３】　前記複数の機器は予め定められたグループに属しており、

前記利用権管理部は、前記グループに属する１台の前記機器からの設定要求に応答して、グループに属する各機器により共有される利用権情報を前記利用権ＤＢに登録する、請求項２に記載の利用権管理装置。

【請求項４】　配信対象となるコンテンツデータを蓄積するコンテンツデータベース（以下、コンテンツＤＢと称する）をさらに備え、

前記機器が送信する設定要求はさらに、取得対象のコンテンツデータを特定しており、

前記機器からの設定要求に応答して、コンテンツＤＢから、取得対象のコンテンツデータを読み出すコンテンツ管理部と、

前記コンテンツ管理部で読み出されたコンテンツデータを暗号化するコンテンツ暗号化部と、

前記コンテンツ暗号化部で暗号化されたコンテンツデータを含む送信データを生成する送信データ生成部とをさらに備え、

前記通信部はさらに、前記送信データ生成部で生成されたデータを、設定要求を送信した機器に送信する、請求項２に記載の利用権管理装置。

【請求項５】　前記コンテンツ暗号化部で暗号化されるコンテンツデータを復号するための復号鍵を含む復号鍵データベース（以下、復号鍵ＤＢと称する）をさらに備え、

前記ライセンス情報生成部は、前記復号鍵ＤＢ内の復号鍵をさらに含むライセンス情報を生成する、請求項１に記載の利用権管理装置。

【請求項６】　前記復号鍵ＤＢ内の復号鍵を、発行要求を送信した機器に関連する情報で暗号化する復号鍵暗号化部をさらに備え、

前記ライセンス情報生成部は、前記復号鍵暗号化部で暗号化された復号鍵をさらに含むライセンス情報を生成する、請求項５に記載の利用権管理装置。

【請求項７】　前記ライセンス情報生成部は、

前記利用権管理部で生成された利用許可情報に基づいて、ライセンス情報の改竄を防止するためのハッシュ値を生成するハッシュ値生成部と、

前記ハッシュ値生成部で生成されたハッシュ値を、前記利用権管理部で生成された利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項１に記載の利用権管理装置。

【請求項８】　前記利用権管理部は、発行要求の送信元となる機器のために利用許可情報を生成できない場合には、利用拒否情報を生成し、

前記通信部はさらに、前記利用権管理部で生成された利用拒否情報を、発行要求の送信元のなる機器に送信する、請求項１に記載の利用権管理装置。

【請求項９】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）と、

前記ユーザ情報ＤＢに未登録の機器識別子を有する機器からの登録要求に応答して、受信登録要求に含まれる未登録の機器識別子を前記ユーザ情報ＤＢに登録するユーザ情報管理部とをさらに備える、請求項１に記載の利用権管理装置。

【請求項１０】　前記ユーザ情報管理部は、１グループに登録されている機器識別子数が、予め定められた上限値以上である場合には、登録要求に応答して、前記ユーザ情報ＤＢへの登録を拒否するための登録拒否通知を生成し、

前記通信部はさらに、前記ユーザ情報管理部で生成された登録拒否通知を、登録要求の送信元となる機器に送信する、請求項９に記載の利用権管理装置。

【請求項１１】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに登録済の機器は、自身の機器識別子を登録対象識別子として少なくとも含む仮登録要求を送信し、

受信仮登録要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに仮登録するユーザ情報管理部をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、登録対象識別子と、仮登録要求の送信元となった機器の機器識別子である登録済識別子とを少なくとも含む本登録要求を送信し、

前記ユーザ情報管理部は、受信本登録要求に含まれる登録対象識別子および登録済識別子に基づいて、前記ユーザ情報ＤＢに仮登録された登録対象識別子を本登録する、請求項１に記載の利用権管理装置。

【請求項１２】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、自身の機器識別子を登録対象識別子として含み、さらに、登録済の機器識別子を含むパスワード要求を送信し、

受信パスワード要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに仮登録し、さらに、未登録の機器に対するパスワードを発行するユーザ情報管理部をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、登録対象識別子と、前記ユーザ情報管理部により発行されたパスワードとを含む登録要求を送信し、

前記ユーザ情報管理部は、受信登録要求に含まれるパスワードと登録対象識別子とに基づいて、前記ユーザ情報ＤＢに仮登録された登録対象識別子を本登録する、請求項１に記載の利用権管理装置。

【請求項１３】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、自身の機器識別子を登録対象識別子として少なくとも含む第１の登録要求を、ユーザ情報ＤＢに登録済の機器に送信し、

前記ユーザ情報ＤＢに登録済の機器は、自身の機器識別子を登録済識別子として含み、さらに、受信した第１の登録要求に含まれる登録対象識別子を含む第２の登録要求を送信し、

受信した第２の登録要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに登録するユーザ情報管理部をさらに備える、請求項１に記載の利用権管理装置。

【請求項１４】　前記利用権ＤＢには、利用権情報と、その利用権情報を利用可能な機器の機器識別子とが登録されており、

予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）と、

各前記機器からの削除要求に応答して、前記ユーザ情報ＤＢおよび前記利用権ＤＢから機器識別子を削除する機器識別子削除部とをさらに備える、請求項１に記載の利用権管理装置。

【請求項１５】　前記複数の機器は予め定められたグループに属しており、

前記利用権管理部は、

前記グループに属する第１の機器からの設定要求に応答して、設定要求の送信元となる第１の機器の利用権情報を前記利用権ＤＢに登録し、

前記グループに属する第２の機器からの設定要求に応答して、設定要求の送信元となる第２の機器を、第１の機器の利用権情報と共有可能に前記利用権ＤＢに登録する、請求項２に記載の利用権管理装置。

【請求項１６】　伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、

前記機器は、

自身を一意に特定するメディア識別子を格納する可搬型記録媒体をデータ通信可能に接続するインターフェイスと、

前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、

前記識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、

前記発行要求生成部から受け取る発行要求を、前記伝送路を通じて、前記利用権管理装置に送信する第１の通信部とを備え、

前記利用権管理装置は、

前記可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、前記機器からの発行要求に応答して、前記可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信し、

前記機器はさらに、

前記利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える、機器。

【請求項１７】　前記利用権管理装置は、前記機器がコンテンツデータを利用するための最低限度の利用許可情報を生成する利用権管理部を備える、請求項１６に記載の機器。

【請求項１８】　前記利用権管理装置は、

ライセンス情報を生成するために、前記利用権管理部で生成された利用許可情報に基づいて、第１のハッシュ値を生成する第１のハッシュ値生成部と、

前記第１のハッシュ値生成部から受け取る第１のハッシュ値を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項１７に記載の機器。

【請求項１９】　前記ライセンス情報処理部は、

受信ライセンス情報に含まれる利用許可情報に基づいて、第２のハッシュ値を生成する第２のハッシュ値生成部と、

前記第１の通信部から受け取るライセンス情報に含まれる第１のハッシュ値と、前記第２のハッシュ値生成部から受け取る第２のハッシュ値とに基づいて、

前記第１の通信部から受け取るライセンス情報に含まれる利用許可情報が改竄されているか否かを判定する改竄判定部とを含む、請求項１８に記載の機器。

【請求項２０】　前記コンテンツデータは、前記機器に、予め定められた暗号鍵で暗号化された状態で配信され、

前記ライセンス情報組立部はさらに、前記利用権管理部から受け取る発行要求からメディア識別子を取り出し、

前記利用権管理装置は、

前記暗号鍵で暗号化されたコンテンツデータを復号可能な復号鍵を管理する復号鍵管理部と、

前記復号鍵管理部で管理される復号鍵を、前記ライセンス情報組立部により取り出されたメディア識別子で暗号化する復号鍵暗号化部とをさらに備え、

前記ライセンス情報組立部はさらに、前記復号鍵暗号化部から受け取る暗号化された復号鍵を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てる、請求項１８に記載の機器。

【請求項２１】　前記ライセンス情報処理部は、前記識別子抽出部から受け取るメディア識別子を使って、前記第１の通信部から受け取るライセンス情報に含まれる暗号化された復号鍵を復号する復号鍵復号部をさらに備える、請求項２０に記載の機器。

【請求項２２】　自身に割り当てられた機器識別子を格納するための機器識別子格納部をさらに備え、

前記識別子抽出部は、ユーザの操作に応じて、前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出すか、前記機器識別子格納部から機器識別子を取り出すかを決定する、請求項１６に記載の機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、利用権管理装置に関し、より特定的には、コンテンツデータに関連する権利を管理する利用権管理装置に関する。

【０００２】

【従来の技術】近年、ネットワークのブロードバンド化および常時接続環境により、コンテンツ配信システムが身近なものになりつつある。また、このようなコンテンツ配信システムの普及には、コンテンツデータに関連する権利の保護が重要であることから、従来から、様々な権利管理技術の研究および開発がなされている。ここで、本願明細書では、著作権または販売権のようなコンテンツデータに関連する権利を、デジタルライツと称する。以下、従来の権利管理技術を組み込んだコンテンツ情報配信システムについて説明する。

【０００３】従来のコンテンツ配信システムには、コンテンツ配信装置と、パーソナルコンピュータ（以下、ＰＣと略記する）とが、インターネットに代表されるネットワークにより、データ通信可能に接続される。コンテンツ配信装置は、コンテンツデータ、コンテンツ復号鍵および利用条件データの組みを少なくとも１つ格納している。コンテンツデータは、例えば、音楽に代表されるコンテンツを表すデジタルデータであり、予め定められた方式で暗号化される。コンテンツ復号鍵は、暗号化されたコンテンツデータを復号するための鍵である。利用条件データは、上述のコンテンツデータの利用可能な条件（以下、利用条件と称する）を表すデータである。利用条件としては、コンテンツデータの利用回数が代表的である。ＰＣは、上述のコンテンツデータをコンテンツ配信装置から取得し、さらに、取得したコンテンツデータを利用するために必要なコンピュータプログラム（以下、単にプログラムと称する）を格納している。

【０００４】以上のコンテンツ配信システムでは、以下のようにして、コンテンツデータが配信される。まず、ＰＣは、予め格納されているプログラムを実行して、コンテンツデータの配信をコンテンツ配信装置に要求する。コンテンツデータの要求は、一般的に、コンテンツ特定情報および端末固有情報を、ＰＣがネットワークを介してコンテンツ配信装置に送信することで行われる。コンテンツ特定情報は、上述のコンテンツデータを一意に特定する情報である。端末固有情報は、ＰＣにより予め保持されており、上述のコンテンツデータの要求元であるＰＣを一意に特定可能な情報である。

【０００５】コンテンツ配信装置は、ＰＣからの要求に応答して、上述のコンテンツ復号鍵を、今回受信した端末固有情報を使って暗号化する。その後、コンテンツ配信装置は、上述の暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵と、利用条件データとをＰＣに送信する。ＰＣは、コンテンツ配信装置により配信されたコンテンツデータ、コンテンツ復号鍵および利用条件データを受信し、内部に備える記憶装置に格納する。

【０００６】以上の格納後、ＰＣのユーザは、コンテンツデータを復号することで、それが表すコンテンツを出力可能な状態になる。実際にコンテンツを出力するまでには、ユーザは最初に、その旨をＰＣに指示する。この指示に応答して、ＰＣは、以下のように動作する。ＰＣは、記憶装置内の利用条件データにより表される利用条件に、今回の利用が合致しているか否かを判定する。ＰＣは、利用条件に合致する場合に限り、以下の処理を実行する。次に、記憶装置内のコンテンツ復号鍵は暗号化されているので、ＰＣは、自身が保持する端末固有情報を使って、当該コンテンツ復号鍵を復号する。さらに、記憶装置内のコンテンツデータもまた上述のように暗号化されているので、ＰＣは、復号したコンテンツ復号鍵を使って、当該コンテンツデータを復号した後、それが表すコンテンツを再生し出力する。

【０００７】以上のコンテンツ配信システムでは、権利管理技術としてのＤＲＭ(Digital Rights Management)

により、デジタルライツが保護されている。ＤＲＭによるデジタルライツの保護は、以下の３つの技術により実現される。第１の保護技術は、コンテンツ配信装置は、暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵を送信する。ここで、コンテンツ復号鍵は、コンテンツデータを要求したＰＣ以外では復号できない。それゆえ、たとえ、暗号化されたコンテンツデータが他のＰＣに転送されたとしても、他のＰＣは、コンテンツ復号鍵の暗号を解くことができず、その結果、コンテンツデータを再生することができない。以上のことから、ＤＲＭでは、コンテンツ復号鍵は、唯一のＰＣに括り付けられると言える。これにより、デジタルライツが保護される。

【０００８】第２の保護技術は耐タンパ技術である。つまり、ＰＣには、各暗号を解くための復号プログラムが必要となるが、当該復号プログラムの解析は、上述の耐タンパ技術により防止される。これによっても、デジタルライツが保護される。

【０００９】第３に、上述したように、従来のコンテンツ配信システムでは、コンテンツ配信装置は、利用条件データをＰＣに送信する。ＰＣは、受信した利用条件データを管理する。そして、ＰＣは、コンテンツデータの利用毎に、自身が管理する利用条件データが表す利用条件をチェックし、今回の利用が利用条件に合致していない場合には、それ以降の処理を行わない。これによっても、デジタルライツが保護される。

【００１０】

【発明が解決しようとする課題】近年、セットトップボックス、テレビジョン受像機、音楽再生機およびゲーム機器に代表されるＰＣ以外の民生機器にもネットワーク接続機能が付加されるようになってきた。これによって、民生機器が上述のコンテンツ配信装置からコンテンツデータを受信できるようになり、さらには、複数の民生機器の間でデータ通信ができるようになってきた。以上のことから、民生機器にも権利管理技術が組み込まれることが望まれる。しかしながら、上述のＤＲＭのような権利管理技術を民生機器に組み込むことは、以下の問題点を想定できるため得策ではない。

【００１１】第１に、コンテンツ復号鍵は、唯一のＰＣに括り付けられるため、ＰＣおよび他の民生機器の利用者が同一であっても、他の民生機器は、そのコンテンツ復号鍵を使って、コンテンツデータを復号することができないという問題点があった。このような問題点ゆえ、利用者は、コンテンツデータを利用する際には、コンテンツ鍵を利用できるＰＣを使わなければならないため、従来の権利管理技術は、利用者にとって使い勝手の良いものではなかった。

【００１２】第２に、上述のＤＲＭには、耐タンパ技術が組み込まれ、さらに、ＰＣがコンテンツデータを再生する前に必ず、内部に格納した利用条件データに基づいて、当該コンテンツデータを利用可能か否かをチェックする。このように耐タンパ技術は上述のＰＣに大きな処理負担を強いる。しかしながら、ＰＣは、例えば、ビデオ再生、オーディオ再生またはゲームプレイ等、汎用的な用途に使えるよう、相対的に高性能なハードウェアを実装している。それゆえ、ＰＣにＤＲＭを組み込んでも、さほど問題にはならない。それに対して、民生機器に求められるのは低価格であり、さらに、民生機器は、ビデオ再生、オーディオ再生およびゲームプレイのそれぞれに特化した用途に使用されることが一般的である。以上の観点から、民生機器には、ＰＣほど高性能なハードウェアが実装されておらず、大きな処理負担を要求するＤＲＭを組み込むのは困難であるという問題点があった。

【００１３】それ故に、本発明の第１の目的は、複数の民生機器が共通のデジタルライツを共有できる権利管理技術を提供することである。また、本発明の第２の目的は、民生機器に適した権利管理技術を提供することである。

【００１４】

【課題を解決するための手段および発明の効果】上記第１の目的を達成するために、本願の第１の発明は、複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権ＤＢと称する）と、各機器からの発行要求に応答して、利用権ＤＢに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える。

【００１５】上記のように第１の発明によれば、利用権情報は、複数の機器に割り当てられるので、複数の機器が共通の利用権情報を共有可能な権利保護技術を提供することが可能となる。

【００１６】上記第２の目的を達成するために、本願の第２の発明は、伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、可搬型記録媒体は、自身を一意に特定するメディア識別子を格納しており、機器は、可搬型記録媒体をデータ通信可能に接続するインターフェイスと、インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、発行要求生成部から受け取る発行要求を、伝送路を通じて、利用権管理装置に送信する第１の通信部とを備

える。ここで、利用権管理装置は、可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、機器からの発行要求に応答して、可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信する。機器はさらに、利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える。

【００１７】上記のように第２の発明によれば、コンテンツデータの利用権情報を利用権管理装置側で管理しているので、機器に、利用権情報のためにかかる処理負担を負わせる必要が無くなる。これによって、相対的に処理能力の低い機器に適した権利保護技術を提供することが可能となる。

【００１８】さらに、第２の発明によれば、機器において、識別子抽出部は、機器に接続された可搬型記録媒体から、メディア識別子を取り出す。さらに、発行要求生成部は、取り出されたメディア識別子を使って発行要求を生成することができる。これによって、可搬型記録媒体のユーザは、自分の利用権情報を使って、他者の機器上でコンテンツデータを利用することが可能となる。

【００１９】

【発明の実施の形態】「第１の実施形態」図１は、本発明の第１の実施形態に係る利用権管理装置１１を収容したライセンス情報管理システムＳａの全体構成を示すブロック図である。図１において、ライセンス情報管理システムＳａは、利用権管理装置１１と、複数の機器２１の一例として２つの機器２１ａおよび２１ｂと、伝送路３１とを備えている。利用権管理装置１１は、コンテンツ配信に関わる事業者α側に設置される。また、機器２１ａおよび２１ｂは、典型的には、事業者αとの契約に基づいてコンテンツ配信を受ける契約者βにより使用される。また、伝送路３１は、有線または無線であり、利用権管理装置１１と、機器２１ａまたは機器２１ｂとをデータ通信可能に接続する。

【００２０】次に、図２を参照して、図１の利用権管理装置１１の詳細な構成について説明する。図２において、利用権管理装置１１は、コンテンツデータベース１１１と、復号鍵データベース１１２と、ユーザ情報データベース１１３と、利用権データベース１１４と、通信部１１５と、ユーザ認証部１１６と、利用権管理部１１７と、コンテンツ管理部１１８と、コンテンツ暗号化部１１９と、送信データ生成部１２０と、ライセンス情報生成部１２１と、復号鍵管理部１２２と、復号鍵暗号化部１２３とを備えている。また、ライセンス情報生成部１２１は、より詳しくは、図３に示すように、ハッシュ値生成部１２１１と、ライセンス情報組立部１２１２とを含んでいる。

【００２１】次に、図４を参照して、図１の機器２１ａおよび２１ｂの詳細な構成について説明する。図４において、機器２１ａおよび２１ｂは、典型的には、パーソナルコンピュータ（以下、ＰＣと称する）、セットトップボックス、音楽再生機、テレビジョン受像機およびゲーム機のいずれかである。ただし、本実施形態では、便宜上、機器２１ａおよび２１ｂは、それぞれが音楽再生機能を有するＰＣおよび音楽再生機であると仮定する。この仮定下では、機器２１ａおよび２１ｂのそれぞれは少なくとも、機器識別子格納部２１１と、設定要求生成部２１２と、通信部２１３と、コンテンツ管理部２１４と、コンテンツ蓄積部２１５と、発行要求生成部２１６と、ライセンス情報処理部２１７と、コンテンツ復号部２１８と、コンテンツ再生部２１９とを備えている。また、ライセンス情報処理部２１７は、より詳しくは、図５に示すように、改竄判定部２１７１と、ハッシュ値生成部２１７２と、利用許可判定部２１７３と、復号鍵復号部２１７４とを含んでいる。

【００２２】次に、上記ライセンス情報管理システムＳａにおいて、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。この準備作業では、図２のコンテンツデータベース（以下、コンテンツＤＢと称す）１１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）１１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢと称す）１１３とが事業者αにより構築される。

【００２３】まず、図６（ａ）を参照して、図２のコンテンツＤＢ１１１について詳細に説明する。まず、事業者αは、契約者βに配信されるコンテンツデータＤｃｎｔを、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータＤｃｎｔは、機器２１ａおよび２１ｂの両方で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータＤｃｎｔは、ゲームプログラムまたはアプリケーションソフトウェアであっても良い。ただし、便宜上、本実施形態では、コンテンツデータＤｃｎｔは音楽を表すデータであると仮定する。

【００２４】事業者αは、以上のようにして得たコンテンツデータＤｃｎｔのそれぞれに、コンテンツ識別子Ｉｃｎｔを割り当てる。コンテンツ識別子Ｉｃｎｔは好ましくは、本ライセンス情報管理システムＳａにおいてコンテンツデータＤｃｎｔを一意に特定する情報である。さらに、コンテンツ識別子Ｉｃｎｔは、コンテンツデータＤｃｎｔの格納場所を示すロケータでもあることが好ましい。また、以上のコンテンツデータＤｃｎｔは、デジタルライツを保護する観点から、利用権管理装置１１側で暗号化された状態で機器２１ａまたは２１ｂに配信される。そのため、事業者αは、各コンテンツデータＤｃｎｔに専用の暗号鍵Ｋｅを割り当てる。以上のコンテンツ識別子Ｉｃｎｔ、コンテンツデータＤｃｎｔおよび暗号鍵Ｋｅの組み合わせがコンテンツＤＢ１１１に蓄積される。したがっ

て、図６（ａ）に示すように、コンテンツＤＢ１１１は、コンテンツ識別子Ｉｃｎｔ、コンテンツデータＤｃｎｔおよび暗号鍵Ｋｅの組み合わせの集まりとなる。コンテンツＤＢ１１１において、コンテンツ識別子Ｉｃｎｔは特に、同じ組みのコンテンツデータＤｃｎｔを一意に特定する。また、暗号鍵Ｋｅは、同じ組みのコンテンツデータＤｃｎｔを暗号化するために使用される。

【００２５】また、本実施形態では、図示の簡素化するため、コンテンツＤＢ１１１は、コンテンツ識別子Ｉｃｎｔ、コンテンツデータＤｃｎｔおよび暗号鍵Ｋｅから構成されるとして説明するが、コンテンツデータＤｃｎｔおよび暗号鍵Ｋｅ毎のデータベースが構築されてもよい。また、コンテンツ識別子Ｉｃｎｔは、コンテンツデータＤｃｎｔのロケータであることが好ましい。このような場合、利用権管理装置１１ａ、機器２１ａまたは２１ｂの設定要求Ｄｒｒａに含まれるコンテンツ識別子Ｉｃｎｔを使って、コンテンツＤＢ１１１からコンテンツデータＤｃｎｔを読み出せるので、コンテンツＤＢ１１１に、コンテンツ識別子Ｉｃｎｔを登録しておく必然性はない。

【００２６】次に、図６（ｂ）を参照して、図２の復号鍵ＤＢ１１２について詳細に説明する。上述のように、各コンテンツデータＤｃｎｔは暗号鍵Ｋｅで暗号化された状態で機器２１ａまたは２１ｂに送信される。ここで、以下の説明では、暗号鍵Ｋｅで暗号化されたコンテンツデータＤｃｎｔを、暗号済みコンテンツデータＤｅｃｎｔと称する。暗号済みコンテンツデータＤｅｃｎｔの復号のためには、暗号鍵Ｋｅに対応する復号鍵Ｋｄが、機器２１ａまたは２１ｂに提供される必要がある。この必要性から、事業者αは、コンテンツＤＢ１１１内の各暗号鍵Ｋｅに対応する復号鍵Ｋｄを準備する。ここで、復号鍵Ｋｄは、暗号鍵Ｋｅと同じビット列からなっていてもよいし、異なるビット列からなっていてもよい。以上の復号鍵Ｋｄは、上述のコンテンツ識別子Ｉｃｎｔと共に、復号鍵ＤＢ１１２に登録される。以上のことから、復号鍵ＤＢ１１２は、図６（ｂ）に示すように、コンテンツ識別子Ｉｃｎｔおよび復号鍵Ｋｄの組み合わせの集まりとなる。復号鍵ＤＢ１１２において、コンテンツ識別子Ｉｃｎｔは特に、同じ組みの復号鍵Ｋｄに割り当てられているコンテンツデータＤｃｎｔを特定する。また、復号鍵Ｋｄは、同じ組みのコンテンツ識別子Ｉｃｎｔで特定される暗号済みコンテンツデータＤｅｃｎｔを復号するために使用される。

【００２７】次に、図７（ａ）を参照して、図２のユーザ情報ＤＢ１１３について詳細に説明する。上述のように、契約者βは、事業者αとコンテンツ配信に係る契約を交わす。ここで、両者の契約に関しては、契約者βが伝送路３１を通じて事業者αと行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者αは、契約者βが所有する複数の機器２１（つまり、機器２１ａおよび２１ｂ）のそれぞれに機器識別子Ｉｄｖを割り当てる。ここで、図１に示すように、本実施形態では、機器２１ａと２１ｂとが例示されているから、事業者αは、それぞれの機器識別子Ｉｄｖとして機器識別子ＩｄｖａおよびＩｄｖｂを割り当てる。機器識別子ＩｄｖａおよびＩｄｖｂは、ライセンス情報管理システムＳａにおいて、契約者β側の機器２１ａおよび２１ｂを一意に特定する。以上の機器識別子ＩｄｖａおよびＩｄｖｂが、ユーザ情報ＤＢ１１３に登録される。さらに、事業者αは、契約者βおよびその関係者が、機器２１ａおよび２１ｂのいずれを使っても、コンテンツデータＤｃｎｔを利用できるように、グループ識別子Ｉｇｐを、契約者βとの契約に割り当てる。ここで、契約者βおよびその関係者を包括的に述べることができるように、これらをユーザβと称する。以上の機器識別子ＩｄｖａおよびＩｄｖｂと、グループ識別子Ｉｇｐとを使って、事業者αは、ユーザ情報ＤＢ１１３を構築する。

【００２８】より具体的には、ユーザ情報ＤＢ１１３は、図７（ａ）に示すように、複数の契約者レコードＲｃｓの集まりである。契約者レコードＲｃｓは、１契約毎に作成され、典型的には、グループ識別子Ｉｇｐと、機器識別子数Ｎｄｖと、複数の機器識別子Ｉｄｖとを含む。グループ識別子Ｉｇｐは、契約者レコードＲｃｓに含まれる複数の機器識別子Ｉｄｖが同一のグループに属することを特定する。機器識別子数Ｎｄｖは、グループ識別子Ｉｇｐで特定されるグループに属する機器２１の数を示す。各機器識別子Ｉｄｖは、グループ識別子Ｉｇｐで特定されるグループに属する各機器２１を特定する。以上の契約者レコードＲｃｓにより、利用権管理装置１１は、複数の機器２１が同一グループに属することを把握することができる。なお、もし、契約者が１台の機器２１しか使わない場合には、契約者レコードＲｃｓは、それに割り当てられた機器識別子Ｉｄｖのみを含んでいれば良い。

【００２９】ここで図４を再度参照する。事業者αにより割り当てられた機器識別子ＩｄｖａおよびＩｄｖｂはさらに、ユーザβ側の機器２１ａおよび２１ｂにおける機器識別子格納部２１１に設定される。ここで注意を要するのは、図４では機器識別子Ｉｄｖａおよび Ｉｄｖｂの双方が機器識別子格納部２１１に格納されるように見えるが、そうではなく、機器２１ａの機器識別子格納部２１１には機器識別子Ｉｄｖａが設定され、機器２１ｂの機器識別子格納部２１１には機器識別子Ｉｄｖｂが設定される。また、以上の機器識別子ＩｄｖａおよびＩｄｖｂの設定に関しては、例えば、事業者αがユーザβ側の機器２１ａまたは２１ｂを操作して設定する。また、他にも、事業者α側が、伝送路３１を通じて、契約者βに割り当てた機器識別子ＩｄｖａまたはＩｄｖｂを機器２１ａまたは２１ｂに送信し、それぞれが、受信した機器識別子ＩｄｖａまたはＩｄｖｂを、それぞれの機器識別子格納部２１１に自動的に設定するようにしてもよい。さらに、以上の機器識別子ＩｄｖａおよびＩｄｖｂは、機器２１ａまたは２１ｂの工

場出荷時に、それぞれの機器識別子格納部２１１に設定されていてもよい。このような場合、契約者βは、契約時に、機器２１ａおよび２１ｂに設定されている機器識別子Ｉｄｖａおよび Ｉｄｖｂを事業者αに告知する。事業者αは、告知された機器識別子Ｉｄｖａおよび Ｉｄｖｂを使って、ユーザ情報ＤＢ１１３を構築する。

【００３０】また、図７（ｂ）には、利用権データベース１１４が示されているが、これについては後述する。

【００３１】以上の準備が終了すると、機器２１ａおよび２１ｂの一方は、ユーザβの操作に従って、利用権管理装置１１に対して、コンテンツデータＤｃｎｔ の利用権を設定することや、コンテンツデータＤｃｎｔ を取得することが可能となる。以下、図８を参照して、コンテンツデータＤｃｎｔ の利用権設定および取得時における、機器２１ａおよび利用権管理装置１１０の間のデータ通信について説明する。まず、ユーザβは、機器２１ａを操作して、利用権管理装置１１にアクセスし、コンテンツＤＢ１１１内のコンテンツデータＤｃｎｔ から、今回取得したいもののコンテンツ識別子Ｉｃｎｔ を特定する。以降の説明において、今回指定されたコンテンツデータＤｃｎｔ を、取得対象コンテンツデータＤｃｎｔ と称する。さらに、ユーザβは、取得対象コンテンツデータＤｃｎｔ を利用する際の利用条件Ｃｃｎｔ を指定する。

【００３２】以下、利用条件Ｃｃｎｔ について、より詳細に説明する。利用条件Ｃｃｎｔ は、どのような条件で、機器２１ａがコンテンツデータＤｃｎｔ の利用権の設定を要求するのかを示す情報である。コンテンツデータＤｃｎｔ が音楽を表す場合、利用条件Ｃｃｎｔ としては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ｃｃｎｔ は、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、２つ以上の組み合わせであってもよい。利用条件Ｃｃｎｔ としての有効期間は、例えば、２００１年６月１日から２００１年８月３１日までと設定され、設定された期間に限り、機器２１ａは、コンテンツデータＤｃｎｔ を再生できる。再生回数は、例えば、５回と設定され、設定された回数に限り、機器２１ａは、コンテンツデータＤｃｎｔ を再生できる。最大連続再生時間は、例えば、１０秒と設定され、１回の再生において設定された時間までであれば、機器２１ａは、コンテンツデータＤｃｎｔ を再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、１０時間と設定され、設定された時間の範囲内であれば、機器２１ａは、コンテンツデータＤｃｎｔ を自由に再生できる。再生品質は、例えば、ＣＤ(Compact Disc)の品質と設定され、機器２１ａは、設定された再生品質でコンテンツデータＤｃｎｔ を再生できる。

【００３３】なお、上述では、コンテンツデータＤｃｎｔ が音楽を表す場合に設定されうる利用条件Ｃｃｎｔ について説明した。しかし、上述のみに限らず、利用条件Ｃｃｎｔ は、コンテンツデータＤｃｎｔ が表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ｃｃｎｔ は、コンテンツデータＤｃｎｔ の再生回数であるとして、以下の説明を続ける。

【００３４】上述したように、ユーザβは、機器２１ａを操作して、コンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ を指定する。この指定に応答して、機器２１ａは、図９（ａ）に示す設定要求Ｄｒｒａ を生成し、利用権管理装置１１に送信する（図８；ステップＳ１１）。設定要求Ｄｒｒａ は、取得対象コンテンツデータＤｃｎｔ の利用権設定を利用権管理装置１１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤｃｎｔ の配信を利用権管理装置１１に要求するための情報でもある。ステップＳ１１をより具体的に説明すると、まず、設定要求生成部２１２（図４参照）は、ユーザβが指定したコンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ を受け取る。また、設定要求生成部２１２は、機器識別子格納部２１１から機器識別子Ｉｄｖａ を受け取る。その後、設定要求生成部２１２は、以上の機器識別子Ｉｄｖａ 、コンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ に、予め保持する設定要求識別子Ｉｒｒを付加して、設定要求Ｄｒｒａ （図９（ａ）参照）を生成する。ここで、設定要求識別子Ｉｒｒは、利用権管理装置１１が設定要求Ｄｒｒａ を特定するために使用される。設定要求生成部２１２は、以上の設定要求Ｄｒｒａ を通信部２１３に渡す。通信部２１３は、受け取った設定要求Ｄｒｒａ を、伝送路３１を通じて、利用権管理装置１１に送信する。

【００３５】利用権管理装置１１（図２参照）において、通信部１１５は、伝送路３１を通じて送信されてくる設定要求Ｄｒｒａ を受信して、ユーザ認証部１１６に渡す。ユーザ認証部１１６は、設定要求Ｄｒｒａ を受け取ると、その送信元の機器２１ａが契約ユーザβの物であるか否かを判定するためのユーザ認証処理を行う（図８；ステップＳ１２）。より具体的には、ユーザ認証部１１６は、上述のユーザ情報ＤＢ１１３（図７（ａ）参照）にアクセスし、受け取った設定要求Ｄｒｒａ 内の機器識別子Ｉｄｖａ に一致するものが、当該ユーザ情報ＤＢ１１３に登録されているか否かを確認する。ユーザ認証部１１６は、ユーザ情報ＤＢ１１３に一致するものが登録されている場合に限り、今回設定要求Ｄｒｒａ が、ユーザβの機器２１ａから送信されてきたものであると認証する。ユーザ認証部１１６は、以上のユーザ認証が終了すると、受け取った設定要求Ｄｒｒａ を利用権管理部１１７に渡す。

【００３６】なお、契約ユーザβ以外からの設定要求Ｄｒｒａ を受け取った場合、ユーザ認証部１１６は、ユーザ認証に失敗する。この場合、ユーザ認証部１１６は、受信設定要求Ｄｒｒａ を利用権管理部１１７に渡すことなく廃棄する。

【００３７】利用権管理部１１７は、ユーザ認証部１１

６からの受信情報に設定されている設定要求識別子Ｉｒｒを判定することで、今回の受信情報が設定要求Ｄｒｒａであることを認識する。この認識結果に従って、利用権管理部１１７（図２参照）は、利用権データベース（以下、利用権ＤＢと称する）１１４にアクセスして、利用権ＤＢ１１４への利用権登録処理を行う（ステップＳ１３）。より具体的には、利用権管理部１１７は、受信設定要求Ｄｒｒａから機器識別子Ｉｄｖａおよびコンテンツ識別子Ｉｃｎｔを取り出して、これらを含む利用権レコードＲｒｇｔが利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ１３１）。今、利用権ＤＢ１１４には対象となる利用権レコードＲｒｇｔが未登録であると仮定すると、利用権管理部１１７は、ステップＳ１３２を実行する。なお、ステップＳ１３１で利用権レコードＲｒｇｔが登録済の場合の動作については、機器２１ｂの動作と共に説明するため、ここではその説明を省略する。

【００３８】ステップＳ１３２において、利用権管理部１１７はまず、受信設定要求Ｄｒｒａから機器識別子Ｉｄｖａ、コンテンツ識別子Ｉｃｎｔおよび利用条件Ｃｃｎｔを取り出した後、ユーザ情報ＤＢ１１３（図７（ａ）参照）にアクセスする。そして、利用権管理部１１７は、今回取り出した機器識別子Ｉｄｖａを含む契約者レコードＲｃｓから、グループ識別子Ｉｇｐならびに全ての機器識別子Ｉｄｖａおよび Ｉｄｖｂを取り出す（ステップＳ１３２）。次に、利用権管理部１１７は、受信設定要求Ｄｒｒａから取り出した機器識別子Ｉｄｖａ、コンテンツ識別子Ｉｃｎｔおよび利用条件Ｃｃｎｔと、ユーザ情報ＤＢ１１３から得たグループ識別子Ｉｇｐならびに機器識別子Ｉｄｖａおよび Ｉｄｖｂとの組み合わせを、利用権レコードＲｒｇｔとして利用権ＤＢ１１４に登録する（ステップＳ１３３）。ここで、利用権管理部１１７は、設定要求Ｄｒｒａ内の利用条件Ｃｃｎｔで機器２１ａが取得対象コンテンツデータＤｃｎｔを利用する権利の付与を要求しているとみなす。以上のことから、利用権管理部１１７は、設定要求Ｄｒｒａから取り出した利用条件Ｃｍｔを利用権情報Ｄｒｇｔとして扱う。つまり、利用権情報Ｄｒｇｔは、利用条件Ｃｃｎｔが示す条件下で、コンテンツデータＤｃｎｔを機器２１ａが利用する権利を示す。

【００３９】以上の登録処理により、利用権ＤＢ１１４は、図７（ｂ）に示すように、グループ識別子Ｉｇｐ、機器識別子Ｉｄｖａおよび Ｉｄｖｂ 、コンテンツ識別子Ｉｃｎｔならびに利用権情報Ｄｒｇｔを含む利用権レコードＲｒｇｔの集まりとなる。これによって、利用権管理部１１７は、契約者βの取得対象コンテンツデータＤｃｎｔ毎に、その利用権を管理する。また、本実施形態の特徴の一つとして、利用権レコードＲｒｇｔに、ユーザ情報ＤＢ１１３から得た全ての機器識別子Ｉｄｖａおよび Ｉｄｖｂを付加することで、機器２１ａからの設定要求Ｄｒｒａにより、機器２１ａおよび２１ｂは、コンテンツデータＤｃｎｔの利用権を共有できるようになる。利用権管理部１１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Ｄｒｒａをコンテンツ管理部１１８に渡す。

【００４０】今回の設定要求Ｄｒｒａには、利用条件Ｃｃｎｔとして「再生ｍ回」（ｍは自然数）が設定されていると仮定すると、図７（ｂ）に示すように、今回新規登録される利用権レコードＲｒｇｔは、「再生ｍ回」という条件が指定された利用権情報Ｄｒｇｔを含むことになる。

【００４１】なお、本ライセンス情報管理システムＳａの技術的特徴とは関係ないが、ステップＳ１３において、利用権管理部１１７は、利用条件情報Ｄｃｒｔの登録毎に、機器識別子Ｉｄｖａが割り当てられている契約者βに、コンテンツデータＤｃｎｔの利用に対する課金を行ってもよい。

【００４２】コンテンツ管理部１１８は、設定要求Ｄｒｒａを受け取ると、コンテンツデータＤｃｎｔおよびそれ専用の暗号鍵Ｋｅの読み出し処理を行う（ステップＳ１４）。より具体的には、コンテンツ管理部１１８は、受信設定要求Ｄｒｒａから、コンテンツ識別子Ｉｃｎｔを取り出す。その後、コンテンツ管理部１１８は、コンテンツＤＢ１１１にアクセスして、取り出したコンテンツ識別子Ｉｃｎｔが割り当てられているコンテンツデータＤｃｎｔおよび暗号鍵Ｋｅを読み出す。以上の読み出し処理が終了すると、コンテンツ管理部１１８は、読み出したコンテンツデータＤｃｎｔおよび暗号鍵Ｋｅをコンテンツ暗号化部１１９に渡す。さらに、コンテンツ管理部１１８は、受け取った設定要求Ｄｒｒａを送信データ生成部１２０に渡す。

【００４３】コンテンツ暗号化部１１９は、コンテンツデータＤｃｎｔの暗号処理を行う（ステップＳ１５）。より具体的には、コンテンツ暗号化部１１９は、受け取ったコンテンツデータＤｃｎｔを、同時に受け取った暗号鍵Ｋｅで暗号化して、前述の暗号済みコンテンツデータＤｅｃｎｔを生成する。コンテンツ暗号化部１１９は、以上の暗号処理が終了すると、暗号済みコンテンツデータＤｅｃｎｔを送信データ生成部１２０に渡す。

【００４４】送信データ生成部１２０は、コンテンツ管理部１１８からの設定要求Ｄｒｒａと、コンテンツ暗号化部１１９からの暗号済みコンテンツデータＤｅｃｎｔとが揃うと、送信データ生成処理を行う（ステップＳ１６）。より具体的には、送信データ生成部１２０は、受信設定要求Ｄｒｒａから、コンテンツ識別子Ｉｃｎｔおよび機器識別子Ｉｄｖａを取り出す。さらに、送信データ生成部１２０は、取り出した機器識別子Ｉｄｖａおよびコンテンツ識別子Ｉｃｎｔを、受け取った暗号済みコンテンツデータＤｅｃｎｔに付加して、図９（ｂ）に示すような、送信データＤｔｒｎａを生成する。送信データ生成部１２０は、以上の送信データ生成処理が終了すると、送信データＤｔｒｎａを通信部１１５に渡す。通信部１１５は、受け取った送信データＤｔｒｎａを、伝送路３１を介して、機器２１ａへと

送信する（ステップＳ１７）。

【００４５】機器２１ａ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくる送信データDtrnaを受信する（ステップＳ１８）。より具体的には、通信部２１３は、それに含まれる機器識別子Idvaとコンテンツ識別子Icntとから、今回、取得対象コンテンツデータDcntを含む自分宛の送信データDtrnaを受信したことを認識する。このような認識結果に従って、通信部２１３は、受信データDtrnaをコンテンツ管理部２１４に渡す。

【００４６】コンテンツ管理部２１４は、受信データDtrna内のコンテンツ識別子Icntおよび暗号済みコンテンツデータDecntを、コンテンツ蓄積部２１５に蓄積する（ステップＳ１９）。つまり、コンテンツ蓄積部２１５には、図１０に示すように、上述の設定要求Drraを使って要求したコンテンツ識別子Icntおよび暗号済みコンテンツデータDecntの組みが、いくつか蓄積されることになる。

【００４７】デジタルライツの保護の観点から、機器２１ａには暗号済みコンテンツデータDecntが配信される。そのため、機器２１ａは、コンテンツデータDcntを利用する場合には、利用権管理装置１１により提供される復号鍵Kdで、暗号済みコンテンツデータDecntを復号する必要がある。ここで、本ライセンス情報管理システムSaでは、復号鍵Kdを機器２１ａに提供するために、ライセンス情報Dlcaが用いられる。以下、図１１～図１３を参照して、ライセンス情報Dlcaの取得およびコンテンツデータDcntの復号時における機器２１ａおよび利用権管理装置１１の動作について説明する。

【００４８】まず、ユーザβは、機器２１ａを操作して、コンテンツ蓄積部２１５に蓄積されている暗号済みコンテンツデータDecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータDecntを、復号対象コンテンツデータDecntと称する。ユーザβによる指定に応答して、機器２１ａは、図１４（ａ）に示すような発行要求Diraを生成し、利用権管理装置１１に送信する（図１１；ステップＳ２１）。発行要求Diraは、上述のライセンス情報Dlcaの発行を利用権管理装置１１に機器２１ａが要求するための情報である。より具体的には、コンテンツ管理部２１４（図４参照）は、契約者βにより特定された復号対象コンテンツデータDecntに付加されているコンテンツ識別子Icntを、コンテンツ蓄積部２１５から取り出して、発行要求生成部２１６に渡す。発行要求生成部２１６は、コンテンツ管理部２１４により取り出されたコンテンツ識別子Icntを受け取る。さらに、発行要求生成部２１６は、機器識別子格納部２１１から機器識別子Idvaを取り出す。その後、発行要求生成部２１６は、機器識別子Idvaおよびコンテンツ識別子Icntの組み合わせに、発行要求識別子Iirを付加して、発行要求Dira（図１４（ａ）参照）を生成する。ここで、発行要求識別子Iirは、利用権管理装置１１が発行要求Diraを特定するために使用される。発行要求生成部２１６は、以上の発行要求Diraを通信部２１３に渡す。通信部２１３は、受け取った発行要求Diraを伝送路３１を通じて、利用権管理装置１１に送信する。

【００４９】利用権管理装置１１において、通信部１１５（図２参照）は、伝送路３１を通じて送信されてくる発行要求Diraを受信して、ユーザ認証部１１６に渡す。ユーザ認証部１１６は、発行要求Diraを受け取ると、ユーザ認証処理を行う（ステップＳ２２）。ステップＳ２２におけるユーザ認証は、ステップＳ１２のそれと同様であるため、詳細な説明を省略する。ユーザ認証部１１６は、ユーザ認証に成功した場合に限り、受信発行要求Diraを利用権管理部１１７に渡す。

【００５０】利用権管理部１１７は、それに設定されている発行要求識別子Iirを確認して、ユーザ認証部１１６から渡されたものが発行要求Diraであることを認識する。この認識結果に従って、利用権管理部１１７は、受け取った発行要求Diraから、機器識別子Idvaおよびコンテンツ識別子Icntを取り出す（ステップＳ２３）。次に、利用権管理部１１７は、取り出した機器識別子Idvaおよびコンテンツ識別子Icntの組み合わせと同じものを含む利用権レコードRrgtが、利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ２４）。

【００５１】利用権管理部１１７は、ステップＳ２４で「Ｙｅｓ」と判断した場合、対象となる利用権レコードRrgtに含まれる利用権情報Drgtを参照して、機器２１ａに利用許可を与えることができるか否か、つまりコンテンツデータDcntの利用権が残っているか否かを判断する（ステップＳ２５）。ステップＳ２５で「Ｙｅｓ」と判断した場合、利用権管理部１１７は、対象となる利用権情報Drgtを参照して、利用許可情報Dlwaを生成する（ステップＳ２６）。利用許可情報Dlwaは、復号対象コンテンツデータDecntの復号許可を機器２１ａに与えるための情報である。また、利用許可情報Dlwaの生成により、機器２１ａの利用権情報Drgtが使われることになるので、ステップＳ２６の次に、利用権管理部１１７は、ステップＳ２６で使われた分だけ利用権情報Drgtを更新する（ステップＳ２７）。なお、ステップＳ２７の実行時点で、全ての利用権情報Drgtが使われた場合には、それを含んでいた利用権レコードRrgtを利用権ＤＢ１１４から削除しても良い。

【００５２】ここで、以上のステップＳ２５～Ｓ２７の処理の具体例について説明する。上述の仮定に従えば、今回対象となる利用権レコードRrgtにおいて、利用権情報Drgtは、図７（ｂ）に示すように、「再生ｎ回」という利用権を表す。したがって、ステップＳ２５にお

いて、利用権管理部１１７は、機器２１ａに対し、復号対象コンテンツデータDecntの再生許可を与えてもよいと判断する。この判断に従って、利用権管理部１１７は、ステップＳ２６で、利用許可情報Ｄlwａを作成する。この時生成される利用許可情報Ｄlwａとしては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のmを超えない自然数であり、例えば、ユーザβが機器２１ａを操作して指定した値である。他にも、ｎは、機器２１ａの処理能力に応じて、利用権管理部１１７側で設定しても良い。また、ステップＳ２６により、機器２１ａが復号対象コンテンツデータDecntを再生する権利をｎ回使うことになる。そのため、ステップＳ２７において、利用権管理部１１７は、利用権情報Drgtを「再生ｍ回」から「再生（ｍ－ｎ）回」に更新する。

【００５３】以上の具体例では、利用権情報Drgtがコンテンツデータ Dcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳａでは、様々な利用権情報Ｄrgt（つまり利用条件Ccnt）を設定することができる。従って、ステップＳ２３からＳ２７までの処理手順は、利用権情報Drgtに応じて適切に規定される必要がある。

【００５４】以上の利用許可情報Ｄlwａを、利用権管理部１１７（図２参照）は、発行要求Ｄiraと一緒に、ライセンス情報生成部１２１に渡す。より具体的には、ライセンス情報生成部１２１は、図３に示すように、ハッシュ値生成部１２１１およびライセンス情報組立部１２１２を含んでいる。ハッシュ値生成部１２１１には、利用許可情報Ｄlwａのみが渡され、また、ライセンス情報組立部１２１２には、利用許可情報Ｄlwａおよび発行要求Ｄiraの双方が渡される。

【００５５】まず、ハッシュ値生成部１２１１は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報Ｄlwａを代入して、利用許可情報Ｄlwａの改竄を防止するするためのハッシュ値Vhsaを生成する（ステップＳ２８）。つまり、ハッシュ値Vhsaは、利用許可情報Ｄlwａをｎ成多項式ｆ（ｘ）に代入した時に得られる解である。以上のようなハッシュ値Vhsaを、ハッシュ値生成部１２１１は、ライセンス情報組立部１２１２に渡す。

【００５６】ライセンス情報組立部１２１２は、受け取った発行要求Ｄiraを復号鍵管理部１２２に渡す。復号鍵管理部１２２（図２参照）は、前述した復号鍵ＤＢ１１２（図６（ｂ）参照）を管理する。復号鍵管理部１２２は、受け取った発行要求Ｄiraに設定されているコンテンツ識別子Ｉcntおよび機器識別子Ｉdvaを取り出す。さらに、復号鍵管理部１２２は、コンテンツ識別子Ｉcntと同じ組みの復号鍵Kdを復号鍵ＤＢ１１２から取り出して、機器識別子Ｉdvaと一緒に復号鍵暗号化部１２３に渡す。復号鍵暗号化部１２３は、受け取った復号鍵Kdを、同時に受け取った機器識別子Ｉdvaを使って暗号化して（ステップＳ２９）、暗号済みの復号鍵Kedaを生成する。以上の暗号済み復号鍵Kedaおよび機器識別子Ｉdvaは、ライセンス情報組立部１２１２に渡される。

【００５７】ライセンス情報組立部１２１２は、発行要求Ｄiraおよび利用許可情報Ｄlwａ、ハッシュ値Vhsaならびに暗号済み復号鍵Kedaのすべてが揃うと、図１４（ｂ）に示すライセンス情報ＤIcaの生成を開始する（図１２；ステップＳ２１０）。より具体的には、ライセンス情報組立部１２１２は、発行要求Ｄiraから、コンテンツ識別子Ｉcntおよび機器識別子Ｉdvaを取り出して、それぞれを、利用許可情報Ｄlwａ、暗号済み復号鍵Kedaおよびハッシュ値Vhsaの組み合わせに付加する。さらに、ライセンス情報組立部１２１２は、予め保持するライセンス情報識別子ＩＩcを、機器識別子Ｉdvaに付加して、ライセンス情報ＤIcaを生成する。以上のライセンス情報ＤIcaは、復号対象コンテンツデータDecntの機器２１ａにおける利用を制御するための情報である。また、ライセンス情報識別子ＩＩcは、機器２１ａがライセンス情報ＤIcaを特定するための情報である。また、以上のライセンス情報ＤIcaは、通信部１１５および伝送路３１を通じて、機器２１ａに送信される（ステップＳ２１１）。

【００５８】機器２１ａ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくるライセンス情報ＤIcaを受信する（ステップＳ２１２）。より具体的には、通信部２１３は、受信情報に含まれる機器識別子Ｉdvaから、自分宛の情報が到着したと判断し、さらに、それに設定されるライセンス情報識別子ＩＩcから、今回、ライセンス情報ＤIcaを受け取ったことを認識する。このような認識結果に従って、通信部２１３は、受け取ったライセンス情報ＤIcaをライセンス情報処理部２１７に渡す。

【００５９】ライセンス情報処理部２１７は、図５に示すように、改竄判定部２１７１と、ハッシュ値生成部２１７２と、利用許可判定部２１７３と、復号鍵復号部２１７４とを含んでいる。通信部２１３からのライセンス情報ＤIcaは、まず、改竄判定部２１７１に渡される。改竄判定部２１７１は、まず、受け取ったライセンス情報ＤIcaから、利用許可情報Ｄlwａおよびハッシュ値Vhsaを取り出し（ステップＳ２１３）、取り出した利用許可情報Ｄlwａを、ハッシュ値生成部２１７２に渡し、ハッシュ値Vhsaをそのまま保持する。ここで、以下の説明において混同が生じないように、ステップＳ２１３で取り出されたハッシュ値Vhsaを、機器２１ａの外部（つまり利用権管理装置１１）で生成されたものであるという観点から、外部ハッシュ値Vehsaと称する。

【００６０】ハッシュ値生成部２１７２は、利用権管理装置１１側のハッシュ値生成部１２１１（図３参照）と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った

利用許可情報ＤＩwa をハッシュ関数ｆ（ｘ）に代入してハッシュ値Ｖhsa を生成する（ステップＳ２１４）。ここでステップＳ２１４で生成されたハッシュ値Ｖhsa を、機器２１ａ の内部で生成されたものであるという観点から、内部ハッシュ値Ｖ'hsaと称する。ハッシュ値生成部２１７２は、以上の内部ハッシュ値Ｖ'hsaを、改竄判定部２１７１に返す。

【００６１】改竄判定部２１７１は、上述の内部ハッシュ値Ｖ'hsaを受け取ると、利用許可情報ＤＩwa が改竄されているか否かを判定する（ステップＳ２１５）。より具体的には、上述の内部ハッシュ値Ｖ'hsaは、ライセンス情報ＤＩca 内の利用許可情報ＤＩwa が改竄されていないという条件で、外部ハッシュ値Vehsaに一致する。そこで、ステップＳ２１５において、改竄判定部２１７１は、受け取った内部ハッシュ値Ｖ'hsaが外部ハッシュ値Vehsaに一致するか否かを判定する。改竄判定部２１７１は、「Ｙｅｓ」と判定した場合には、利用許可情報ＤＩwa が改竄されておらず、今回送信されてきた利用許可情報ＤＩwa が有効であるとみなして、今回受け取ったライセンス情報ＤＩca を利用許可判定部２１７３に渡す。

【００６２】利用許可判定部２１７３は、受け取ったライセンス情報ＤＩca を参照して、復号対象コンテンツデータＤecntの利用が許可されているか否かを判定する（ステップＳ２１６）。利用許可判定部２１７３は、ステップＳ２１６において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報ＤＩca から、暗号済み復号鍵Ｋeda を取り出して、復号鍵復号部２１７４に渡す。

【００６３】ここで、以上のステップＳ２１６の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報ＤＩca の利用許可情報ＤＩwa により、コンテンツデータＤcnt の再生がｎ回だけ許可されている。かかる場合、利用許可判定部２１７３は、ステップＳ２１６において、利用許可情報ＤＩwa に設定される再生回数が１以上であれば、復号対象コンテンツデータＤecntの利用が許可されていると判断して、受け取ったライセンス情報ＤＩca を復号鍵復号部２１７４に渡す。

【００６４】以上の具体例では、利用権情報Ｄrgt がコンテンツデータＤcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳａ では、様々な利用権情報Ｄrgt （つまり利用条件Ｃｃｎｔ）を設定することができる。従って、ステップＳ２１６の処理は、利用権情報Ｄrgt に応じて適切に規定される必要がある。

【００６５】復号鍵復号部２１７４は、利用許可判定部２１７３から暗号済み復号鍵Ｋedaを受け取る。さらに、復号鍵復号部２１７４は、機器識別子格納部２１１から機器識別子Ｉdva を取り出す。その後、復号鍵復号部２１７４は、暗号済み復号鍵Ｋeda を、機器識別子Ｉdva で復号して（ステップＳ２１７）、復号鍵Ｋd をコンテンツ復号部２１８に渡す。

【００６６】ところで、コンテンツ管理部２１４は、以上のステップＳ２１７の次またはそれ以前に（図１２にはステップＳ２１７の直後の例が示されている）、今回の復号対象コンテンツデータＤecntをコンテンツ蓄積部２１５から取り出す（ステップＳ２１８）。取り出された復号対象コンテンツデータＤecntは、コンテンツ復号部２１８に渡される。コンテンツ復号部２１８は、復号鍵復号部２１７４から受け取った復号鍵Ｋd で、復号対象コンテンツデータＤecntを復号して（ステップＳ２１９）、コンテンツデータＤcnt をコンテンツ再生部２１９に渡す。コンテンツ再生部２１９は、受け取ったコンテンツデータＤcnt を再生して、音声出力する（ステップＳ２２０）。これにより、契約者βは、事業者αから購入したコンテンツデータＤcnt が表す音楽を聴くことができる。

【００６７】ここで、図１２のステップＳ２１５を参照する。ステップＳ２１５において、改竄判定部２１７１は、利用許可情報ＤＩwa がＤ改竄されていると判定する場合がある。また、ステップＳ２１６において、利用許可判定部２１７３は、復号対象コンテンツデータＤecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部２１７１および利用許可判定部２１７３は、今回受け取ったライセンス情報ＤＩca を破棄する（図１３；ステップＳ２２１）。以上から明らかなように、本ライセンス情報管理システムＳａ では、有効なライセンス情報ＤＩca を受信した場合にのみ、復号対象コンテンツデータＤecntの復号が許可される。これによって、上述のデジタルライツが保護される。

【００６８】また、図１１のステップＳ２４において、利用権管理部１１７は、利用権レコードＲrgt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ２５において、利用権管理部１１７は、機器２１ａ に利用許可を与えることができないと判断する場合もある。このような場合、利用権管理部１１７は、復号対象コンテンツデータＤecntの利用を拒否することを示す利用拒否情報Ｄrj（図１４（ｃ）参照）を生成して、通信部１１５に渡す。通信部１１５は、受け取った利用拒否情報Ｄrjを、伝送路３１を介して、機器２１ａ に送信する（図１３；ステップＳ２２２）。

【００６９】機器２１ａ （図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくる利用拒否情報Ｄrjを受信する（ステップＳ２２３）。利用拒否情報Ｄrjの受信以降、機器２１ａ では何の処理も行われない。以上から明らかなように、本ライセンス情報管理システムＳａ では、利用権ＤＢ１１４に有効な利用権レコードＲrgt が登録されてない場合には、利用拒否情報Ｄrjが、発行要求Ｄiraの送信元となる機器２１ａ に送信される。これによって、機器２１ａ 側では、復号対象コ

ンテンツデータDecntは復号されない。これによって、上述のデジタルライツが保護される。

【００７０】なお、ステップＳ２４において、利用権管理部１１７は、利用権レコードRrgt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されていないと判断した後、利用権レコードRrgt を新たに生成して、利用権ＤＢ１１４に登録するようにしてもよい。

【００７１】次に、以上の利用権レコードRrgt の登録により、コンテンツデータDcnt の利用権を機器２１ａと共有している機器２１ｂ および利用権管理装置１１の間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、以下の機器２１ｂ の動作は、上述の機器２１ａ の動作とほとんどの部分で同様であるから、その動作説明を簡素化する。まず、ユーザβは、機器２１ｂ を操作して、コンテンツ識別子 Icnt および利用条件Ccnt を指定する。この指定に応答して、機器２１ｂ は、設定要求Drrb を生成し、利用権管理装置１１に送信する（図８；ステップＳ１１）。設定要求Drrb は、設定要求Drra と比較すると、機器識別子 Idva のの代わりに、機器２１ｂ を一意に特定する機器識別子 Idvb を含む点で相違するだけであるから、その詳細な説明を省略する。なお、機器２１bは、自身が利用可能な利用権レコードRrgt が利用権ＤＢ１１４に登録されていることが予め分かっている場合には、利用条件Ccnt を含まない設定要求Drrbを生成しても良い。

【００７２】利用権管理装置１１（図２参照）において、ユーザ認証部１１６は、通信部１１５を通じて、機器２１ｂ からの設定要求Drrb を受け取る。その後、ユーザ認証部１１６は、機器２１ｂ が契約ユーザβの物であるか否かを判定するためのユーザ認証処理を行う（ステップＳ１２）。ユーザ認証部１１６は、ユーザ認証処理が成功した場合に限り、受け取った設定要求Drrb を利用権管理部１１７に渡す。

【００７３】利用権管理部１１７は、今回の受信情報が設定要求Drrb であることを認識すると、ステップＳ１３を行う。ステップＳ１３において、まず、利用権管理部１１７は、受信設定要求Drrb 内の機器識別子 Idvb およびコンテンツ識別子 Icnt を含む利用権レコードRrgt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ１３１）。前述したように、利用権ＤＢ１１４には、機器２１ａ の設定要求Drra に起因して、機器識別子 Idvb およびコンテンツ識別子 Icnt を含む利用権レコードRrgt が登録済である。この場合、利用権管理部１１７は、ステップＳ１３２～Ｓ１３３を行うことなく、今回の設定要求Drrb をコンテンツ管理部１１８に渡す。

【００７４】コンテンツ管理部１１８は、設定要求Drrb の受信後、コンテンツデータDcnt および暗号鍵Ke を読み出して（ステップＳ１４）、それらをコンテンツ暗号化部１１９に渡す。さらに、コンテンツ管理部１１８は、受信設定要求Drrb を送信データ生成部１２０に渡す。コンテンツ暗号化部１１９は、コンテンツデータDcnt の暗号処理を行い（ステップＳ１５）、それが終了すると、暗号済みコンテンツデータDecntと受信設定要求Drrb とを送信データ生成部１２０に渡す。

【００７５】送信データ生成部１２０は、前述したようにして、送信データDtrnb（図９（ｂ）参照）を生成する（ステップＳ１６）。送信データDtrnbは、送信データDtrnaと比較すると、機器識別子 Idva のの代わりに、機器識別子 Idvb を含む点で相違するだけであるから、その詳細な説明を省略する。ステップＳ１６の次に、送信データ生成部１２０は、送信データDtrnbを通信部１１５に渡し、通信部１１５は、前述したように、受け取った送信データDtrnbを機器２１ｂ へと送信する（ステップＳ１７）。

【００７６】機器２１ｂ（図４参照）において、通信部２１３は、送信データDtrnbを受信し（ステップＳ１８）、その後、受信データDtrnbをコンテンツ管理部２１４に渡す。コンテンツ管理部２１４は、受信データDtrnb内のコンテンツ識別子 Icnt および暗号済みコンテンツデータDecntを、コンテンツ蓄積部２１５に蓄積する（ステップＳ１９）。

【００７７】デジタルライツの保護の観点から、機器２１ｂ は、機器２１ａ の場合と同様に、利用権管理装置１１からライセンス情報Dlcb の発行を受けなければ、コンテンツデータDcnt を利用することができない。以下、図１１～図１３を参照して、ライセンス情報Dlcb の取得およびコンテンツデータDcnt の復号時における機器２１ｂ および利用権管理装置１１の動作について説明する。なお、この時の動作は、機器２１ａ および利用権管理装置１１の動作とほとんどの部分で同様であるから、その動作説明を簡素化する。

【００７８】まず、ユーザβは、機器２１ｂ を操作して、コンテンツ蓄積部２１５の中から、復号対象コンテンツデータDecntを指定する。ユーザβの指定に応答して、機器２１ｂ において、発行要求生成部２１６は、発行要求Dirb （図１４（ａ）参照）を生成し、利用権管理装置１１に送信する（図１１；ステップＳ２１）。発行要求Dirb は、発行要求Dira と比較すると、機器識別子 Idva が機器識別子 Idvb に代わる点で相違するだけであるから、その詳細な説明を省略する。発行要求生成部２１６は、以上の発行要求Dirb を通信部２１３に渡す。通信部２１３は、受信発行要求Dirb を利用権管理装置１１に送信する。

【００７９】利用権管理装置１１において、ユーザ認証部１１６（図２参照）は、通信部１１５を通じて、機器２１ｂ が送信した発行要求Dirb を受け取り、その後、ユーザ認証処理を行う（ステップＳ２２）。ユーザ認証部１１６は、ユーザ認証処理が成功した場合に限り、受信発行要求Dirb を利用権管理部１１７に渡す。利用権

管理部１１７は、受信発行要求Ｄｉｒｂ から、機器識別子Ｉｄｖｂ およびコンテンツ識別子Ｉｃｎｔ を取り出し（ステップＳ２３）、その後、取り出した機器識別子Ｉｄｖｂ およびコンテンツ識別子Ｉｃｎｔ の組み合わせと同じものを含む利用権レコードＲｒｇｔ が、利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ２４）。

【００８０】利用権管理部１１７は、ステップＳ２４で「Ｙｅｓ」と判断した場合、対象となる利用権レコードＲｒｇｔ に含まれる利用権情報Ｄｒｇｔ を参照して、機器２１ｂに利用許可を与えることができるか否か、つまりコンテンツデータＤｃｎｔ の利用権が残っているか否かを判断する（ステップＳ２５）。ステップＳ２５で「Ｙｅｓ」と判断した場合、利用権管理部１１７は、対象となる利用権情報Ｄｒｇｔ を使って利用許可情報ＤｌｗｂをＥ生成する（ステップＳ２６）。利用許可情報ＤｌｗｂはＥ、利用許可情報ＤｌｗａとＥ比較すると、機器識別子Ｉｄｖａ が機器識別子Ｉｄｖｂ に代わる点でのみ相違するから、その詳細な説明を省略する。ステップＳ２６の次に、利用権管理部１１７は、ステップＳ２６で使われた分だけ利用権情報Ｄｒｇｔ を更新する（ステップＳ２７）。

【００８１】以上の利用許可情報Ｄｌｗｂ を、利用権管理部１１７（図２参照）は、発行要求Ｄｉｒｂ と一緒に、ライセンス情報生成部１２１に渡す。ライセンス情報生成部１２１において、ハッシュ値生成部１２１１（図３参照）は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報Ｄｌｗｂ を代入して、利用許可情報Ｄｌｗｂ の改竄を防止するするためのハッシュ値Ｖｈｓｂ を生成し（ステップＳ２８）、それをライセンス情報組立部１２１２に渡す。

【００８２】ライセンス情報組立部１２１２は、受け取った発行要求Ｄｉｒｂ を復号鍵管理部１２２に渡す。復号鍵管理部１２２（図２参照）は、前述した復号鍵ＤＢ１１２（図６（ｂ）参照）を管理しており、受信発行要求Ｄｉｒｂ からコンテンツ識別子Ｉｃｎｔ および機器識別子Ｉｄｖｂ を取り出す。さらに、復号鍵管理部１２２は、コンテンツ識別子Ｉｃｎｔ と同じ組みの復号鍵Ｋｄ を復号鍵ＤＢ１１２から取り出して、機器識別子Ｉｄｖｂ と一緒に復号鍵暗号化部１２３に渡す。復号鍵暗号化部１２３は、受け取った復号鍵Ｋｄ を、同時に受け取った機器識別子Ｉｄｖｂ を使って暗号化して（ステップＳ２９）、暗号済み復号鍵Ｋｅｄｂ を生成する。以上の暗号済み復号鍵Ｋｅｄｂ および機器識別子Ｉｄｖｂ は、ライセンス情報組立部１２１２に渡される。

【００８３】ライセンス情報組立部１２１２は、発行要求Ｄｉｒｂ および利用許可情報Ｄｌｗｂ、ハッシュ値Ｖｈｓｂ ならびに暗号済み復号鍵Ｋｅｄｂ のすべてが揃うと、ライセンス情報Ｄｌｃｂ （図１４（ｂ）参照）を生成する（図１２；ステップＳ２１０）。ライセンス情報Ｄｌｃｂ は、ライセンス情報Ｄｌｃａ と比較すると、機器識別子Ｉｄｖａ 、利用許可情報Ｄｌｗａ 、暗号済み復号鍵Ｋｅｄａ およびハッシュ値Ｖｈｓａ が機器識別子Ｉｄｖｂ 、利用許可情報Ｄｌｗｂ 、暗号済み復号鍵Ｋｅｄｂ およびハッシュ値Ｖｈｓｂ に代わる点で相違するだけであるから、その詳細な説明を省略する。以上のライセンス情報Ｄｌｃｂ は、通信部１１５および伝送路３１を通じて、機器２１ｂに送信される（ステップＳ２１１）。

【００８４】機器２１ｂ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくるライセンス情報Ｄｌｃｂ を受信し（ステップＳ２１２）、それをライセンス情報処理部２１７に渡す。ライセンス情報処理部２１７において、改竄判定部２１７１は、受信ライセンス情報Ｄｌｃｂ から、利用許可情報Ｄｌｗｂ およびハッシュ値Ｖｈｓｂ を取り出し（ステップＳ２１３）、取り出した利用許可情報Ｄｌｗｂをに、ハッシュ値生成部２１７２に渡し、ハッシュ値Ｖｈｓｂ を外部ハッシュ値Ｖｅｈｓｂとして保持する。ハッシュ値生成部２１７２は、利用権管理装置１１側と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った利用許可情報Ｄｌｗｂ をハッシュ関数ｆ（ｘ）に代入して、内部ハッシュ値Ｖｌｈｓｂを生成し（ステップＳ２１４）、それを改竄判定部２１７１に返す。

【００８５】改竄判定部２１７１は、前述と同様にして、上述の内部ハッシュ値Ｖｌｈｓｂを受け取ると、それが外部ハッシュ値Ｖｅｈｓｂに一致するか否かを判定し（ステップＳ２１５）、両者が一致する場合には、今回の利用許可情報Ｄｌｗｂ が有効であるとして、受信ライセンス情報Ｄｌｃｂ を利用許可判定部２１７３に渡す。利用許可判定部２１７３は、前述と同様にして、復号対象コンテンツデータＤｅｃｎｔの利用が許可されているか否かを判定し（ステップＳ２１６）、「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報Ｄｌｃｂ から、暗号済み復号鍵Ｋｅｄｂ を取り出して、復号鍵復号部２１７４に渡す。復号鍵復号部２１７４は、利用許可判定部２１７３から暗号済み復号鍵Ｋｅｄｂ を受け取る。さらに、復号鍵復号部２１７４は、機器識別子格納部２１１から機器識別子Ｉｄｖｂ を取り出す。その後、復号鍵復号部２１７４は、暗号済み復号鍵Ｋｅｄｂ を、機器識別子Ｉｄｖｂ で復号して（ステップＳ２１７）、その結果得られる復号鍵Ｋｄ をコンテンツ復号部２１８に渡す。

【００８６】コンテンツ管理部２１４は、今回の復号対象コンテンツデータＤｅｃｎｔをコンテンツ蓄積部２１５から取り出し（ステップＳ２１８）、それをコンテンツ復号部２１８に渡す。コンテンツ復号部２１８は、復号鍵復号部２１７４からの復号鍵Ｋｄ で、復号対象コンテンツデータＤｅｃｎｔを復号して（ステップＳ２１９）、コンテンツデータＤｃｎｔ をコンテンツ再生部２１９に渡す。コンテンツ再生部２１９は、受け取ったコンテンツデータＤｃｎｔ を再生して、音声出力する（ステップＳ２２０）。

【００８７】以上のように本実施形態によれば、利用権

レコードＲｒｇｔ には、複数の機器識別子Ｉｄｖａ およびＩｄｖｂ が記録される。これによって、利用権管理装置１１は、互いに異なる機器２１ａおよび２１ｂから発行要求ＤｉｒａおよびＤｉｒｂ が送信されてきたとしても、利用権レコードＲｒｇｔ を参照することで、同一の利用権情報Ｄｒｇｔ から生成されたライセンス情報Ｄｌｃａ およびＤｌｃｂをそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【００８８】なお、以上の実施形態では、利用権レコードＲｒｇｔ はグループ識別子Ｉｇｐを含んでいたが、これは、機器２１ａ および２１ｂ が同一グループに属することを明確にするためのものである。つまり、グループ識別子Ｉｇｐは、利用権レコードＲｒｇｔ に必須の情報ではない。また、利用権レコードＲｒｇｔ は、機器２１ａ および２１ｂ の機器識別子Ｉｄｖａ およびＩｄｖｂ を含まずに、グループ識別子Ｉｇｐのみを使って、同一グループに属する機器２１ａ および２１ｂ を特定するようにしても良い。

【００８９】また、以上の実施形態では、複数の機器２１の代表例として、２台の機器２１ａ および機器２１ｂを挙げたが、これに限らず、３台以上の機器で、同一の利用権情報Ｄｒｇｔ を共有するようにしても良い。

【００９０】また、以上の実施形態では、図示の都合上、利用権管理装置１１がコンテンツＤＢ１１１を備えると説明したが、これに限らず、コンテンツデータＤｃｎｔ は別のサーバから機器２１ａ および２１ｂ に配信されても良い。

【００９１】また、以上の実施形態では、ユーザ情報ＤＢ１１３に契約時に登録された機器２１ａ および２１ｂが同一の利用権情報Ｄｒｇｔ を共有する例について説明した。しかし、ユーザβ側の機器２１は、必ずしも機器２１ａ および２１ｂ の２台だけでコンテンツ配信を受けるわけではなく、新しく入手した機器２１を使ってコンテンツデータＤｃｎｔ を利用したい場合もある。以下に説明する利用権管理装置１１ａ ～１１ｄ は、上述の利用権管理装置１１の第１～第４の変型例であって、上述のニーズに対応するために提供される。「第１の変型例」

【００９２】図１５は、利用権管理装置１１ａ を収容したライセンス情報管理システムＳａ１の全体構成を示すブロック図である。図１５のライセンス情報管理システムＳａ１は、図１のライセンス情報管理システムＳａ と比較すると、利用権管理装置１１に代えて利用権管理装置１１ａ を備えている点と、機器２１ｃ をさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａ およびＳａ１に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。なお、図１５には、通信ケーブル３２が示されているが、これは第４の変型例で使われる構成であるため、本変型例だけでなく、第２および第３の変型例では、通信ケーブル３２の説明を省略する。

【００９３】利用権管理装置１１ａ は、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図１６に示すように、ユーザ情報管理部１２４と、登録完了生成部１２５とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ａ の間に相違点は無い。それ故、図１６において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【００９４】機器２１ｃ は、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ａ のユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１ａまたは２１ｂ と比較すると、図１７に示すように、登録要求生成部２２０およびグループ識別子格納部２２１をさらに備える点で相違する。それ以外に、両機器２１ａ および２１ｂ と、機器２１ｃ との間には相違点は無い。それ故、図１７において、図４の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。なお、機器２１ｃ の機器識別子格納部２１１には、機器２１ｃ を一意に特定するための機器識別子Ｉｄｖｃ が予め格納されており、グループ情報格納部２２１には、ユーザβに割り当てられたグループ識別子Ｉｇｐが格納されていると仮定する。

【００９５】次に、図１８を参照して、以上のような構成のライセンス情報管理システムＳａ１において、機器２１ｃ をユーザ情報ＤＢ１１３に登録するまでの機器２１ｃ および利用権管理装置１１ａ の動作について説明する。まず、機器２１ｃ は、ユーザβの操作に従って、ユーザβが事業者αから通知されるグループ識別子Ｉｇｐを、グループ識別子格納部２２１に格納する。その後、ユーザβは、機器２１ｃ を操作して、本機器２１ｃ をユーザ情報ＤＢ１１３に登録する旨を指定する。この指定に応答して、機器２１ｃ において、登録要求生成部２２０は、図１９（ａ）に示す登録要求Ｄｒｓｃ を生成し、利用権管理装置１１ａ に送信する（図１８；ステップＳ３１）。登録要求Ｄｒｓｃ は、本機器２１ｃ をユーザ情報ＤＢ１１３に登録するよう利用権管理装置１１ａ に要求するための情報である。ステップＳ３１をより具体的に説明すると、まず、登録要求生成部２２０は、機器識別子格納部２１１から機器識別子Ｉｄｖｃ を取り出し、さらに、グループ識別子格納部２２１からグループ識別子Ｉｇｐを取り出した後、取り出したグループ識別子Ｉｇｐおよび機器識別子Ｉｄｖｃ の組み合わせに、予め保持する登録要求識別子Ｉｒｓを付加して、登録要求Ｄｒｓｃ （図１９（ａ）参照）を生成する。ここで、登録要求識別子Ｉｒｓは、利用権管理装置１１ａ が登録要求Ｄｒｓｃ を特定するために使用される。登録要求生成部２２０は、以上の登録要求Ｄｒｓｃ を通信部２１３に渡す。通信部２１３は、受け取った登録要求Ｄｒｓｃ を、伝送路３１を通じて、利用権管理装置１１ａ に送信する。

【００９６】利用権管理装置１１ａ（図１６参照）において、通信部１１５は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる登録要求識別子Ｉｒｓから、今回の受信情報が登録要求Ｄｒｓｃであることを認識する。この認識結果に従って、通信部１１５は、受信登録要求Ｄｒｓｃを、ユーザ情報管理部１２４に渡す。ユーザ情報管理部１２４は、受信登録要求Ｄｒｓｃからグループ識別子Ｉｇｐを取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出したグループ識別子Ｉｇｐを含む契約者レコードＲｃｓ（図７（ａ）参照）を検索する（ステップＳ３２）。さらに、ユーザ情報管理部１２４は、検索した契約者レコードＲｃｓから機器識別子数Ｎｄｖを取り出す（ステップＳ３３）。

【００９７】次に、ユーザ情報管理部１２４は、取り出した機器識別子数Ｎｄｖが予め定められた上限値Ｖｕｌ以上であるか否かを判断する（ステップＳ３４）。ここで、上限値Ｖｕｌは、ユーザβがユーザ情報ＤＢ１１３に登録可能な機器数の上限値である。ユーザ情報管理部１２４は、ステップＳ３４で、機器識別子数Ｎｄｖが上限値Ｖｕｌ以上でないと判断した場合には、受信登録要求Ｄｒｓｃから機器識別子Ｉｄｖｃを取り出し、取り出したものを対象となる契約者レコードＲｃｓに追加する（ステップＳ３５）。さらに、ユーザ情報管理部１２４は、機器識別子数Ｎｄｖを１だけインクリメントする（ステップＳ３６）。その結果、契約者レコードＲｃｓは、図７（ａ）に示すものから、図２０に示すようなものに更新される。その後、ユーザ情報管理部１２４は、契約者レコードＲｃｓを正しく更新した旨を登録完了生成部１２５に通知し、さらに、受信登録要求Ｄｒｓｃ内の機器識別子Ｉｄｖｃを登録完了生成部１２５に渡す。

【００９８】登録完了生成部１２５は、ユーザ情報管理部１２４から契約者レコードＤｒｓｃの更新が完了したことが通知されると、図１９（ｂ）に示す登録完了通知Ｄｓｃｃを生成し、機器２１ｃに送信する（ステップＳ３７）。登録完了通知Ｄｓｃｃは、本機器２１ｃをユーザ情報ＤＢ１１３に正しく登録したことを機器２１ｃに通知するための情報である。ステップＳ３７をより具体的に説明すると、まず、登録完了生成部１２５は、ユーザ情報管理部１２４から受け取った機器識別子Ｉｄｖｃに、予め保持する登録完了識別子Ｉｓｃを付加して、登録完了通知Ｄｓｃｃ（図１９（ｂ）参照）を生成する。ここで、登録完了識別子Ｉｓｃは、機器２１ｃが登録完了通知Ｄｓｃｃを特定するために使用される。登録完了生成部１２５は、以上の登録完了通知Ｄｓｃｃを通信部１１５に渡す。通信部１１５は、受け取った登録完了通知Ｄｓｃｃを、伝送路３１を通じて、機器２１ｃに送信する。

【００９９】機器２１ｃ（図１７参照）において、通信部２１３は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる登録完了識別子Ｉｓｃから、今回の受信情報が登録完了通知Ｄｓｃｃであることを認識する。この認識結果に従って、通信部２１３は、受信登録完了通知Ｄｓｃｃを、設定要求生成部２１２に渡す。設定要求生成部２１２は、受信情報に設定されている登録完了識別子Ｉｓｃから、今回登録完了通知Ｄｓｃｃを受信したことを認識する（ステップＳ３８）。この認識結果に従って、設定要求生成部２１２は図８のステップＳ１１を実行可能な状態になったと判断し、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様に、利用権管理装置１１ａとデータ通信を行う。

【０１００】以上のように本変型例によれば、利用権管理装置１１ａおよび機器２１ｃのデータ通信により、ユーザβが新しい入手した機器２１ｃの機器識別子Ｉｄｖｃを、ユーザ情報ＤＢ１１３に登録することが可能になるので、より使い勝手の良いライセンス情報管理システムＳａ１を提供できるようになる。

【０１０１】なお、ステップＳ３４において、機器識別子数Ｎｄｖが上限値Ｖｕｌ以上であると判断された場合、ユーザ情報管理部１２４は、ステップＳ３５～Ｓ３６のような処理を行わずに、契約者レコードＲｃｓの更新を拒否する旨を登録完了生成部１２５に通知し、さらに、受信登録要求Ｄｒｓｃ内の機器識別子Ｉｄｖｃを登録完了生成部１２５に渡す。登録完了生成部１２５は、契約者レコードＤｒｓｃの更新拒否が通知されると、図１９（ｃ）に示す登録拒否通知Ｄｓｒｃを生成し、通信部２１３および伝送路３１を通じて、機器２１ｃに送信する（ステップＳ３９）。登録拒否通知Ｄｒｓｃは、本機器２１ｃをユーザ情報ＤＢ１１３に登録できないことを機器２１ｃに通知するための情報であり、ユーザ情報管理部１２４から受け取った機器識別子Ｉｄｖｃと、予め保持する登録拒否識別子Ｉｓｒを含む。機器２１ｃ（図１７参照）において、設定要求生成部２１２は、通信部２１３を通じて、登録拒否通知Ｄｓｒｃを受け取り（ステップＳ３１０）、その通知に従って、設定要求生成部２１２は、図８のステップＳ１１を実行可能な状態ではないと判断し、処理を終了する。

【０１０２】また、ステップＳ３２において、ユーザ情報管理部１２４は、取り出したグループ識別子Ｉｇｐを含む契約者レコードＲｃｓ（図７（ａ）参照）を見つけることができない場合には、ステップＳ３９と同様の処理を行って、機器識別子Ｉｄｖｃのユーザ情報ＤＢ１１３への登録を拒否することが好ましい。

【０１０３】なお、以上の第１の変型例では、機器２１ｃおよび利用権管理装置１１ａがデータ通信を行うことにより、機器識別子Ｉｄｖｃがユーザ情報ＤＢ１１３に登録されていた。しかし、これに限らず、以下の第２～第４の変型例のように、機器２１ｃと、他の機器２１ａまたは機器２１ｂとが協働して、機器識別子Ｉｄｖｃがユーザ情報ＤＢ１１３に登録されるようにしても良い。

【０１０４】「第２の変型例」次に、第２の変型例に係る利用権管理装置１１ｂを収容したライセンス情報管理

システムＳａ2の全体構成について説明する。ライセンス情報管理システムＳａ2は、図１のライセンス情報管理システムＳａと比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｂを備えている点と、機器２１ｃをさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ2に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１０５】利用権管理装置１１ｂは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図２１に示すように、ユーザ情報管理部１２６と、登録完了生成部１２７とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｂの間に相違点は無い。それ故、図２１において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１０６】機器２１ａまたは機器２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉｄａおよび Ｉｄｂは、利用権管理装置１１ｂのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａまたは２１ｂは、機器２１ｃの機器識別子Ｉｄｃの登録のために、図４と比較すると、図２２に示すように、機器識別子入力部２２２と、仮登録要求生成部２２３と、仮登録完了出力部２２４とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａおよび２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図２２において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１０７】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ｂのユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１ａまたは２１ｂと比較すると、図２３に示すように、機器識別子入力部２２５および本登録要求生成部２２６をさらに備える点で相違する。それ以外に、両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図２３において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１０８】次に、図２４および図２５を参照して、以上のような構成のライセンス情報管理システムＳａ2において、機器２１ｃの機器識別子Ｉｄｃをユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｂの動作について説明する。ユーザβは、機器２１ａを操作して、機器識別子Ｉｄｃをユーザ情報ＤＢ１１３に仮登録する旨を指定する。この指定に関連して、機器２１ａの機器識別子入力部２２２は、ユーザβが機器２１ａを操作することにより入力された機器２１ｃの機器識別子Ｉｄｃを、仮登録要求生成部２２３に通知する（図２４；ステップＳ４１）。ここで、以下の説明では、機器２１ｃの機器識別子Ｉｄｃを登録対象識別子Ｉｄｃと称する。仮登録要求生成部２２３は、上述の通知に応答して、図２６（ａ）に示す仮登録要求Ｄｐｒｓｃを生成し、利用権管理装置１１ｂに送信する（ステップＳ４２）。仮登録要求Ｄｐｒｓｃは、登録対象識別子Ｉｄｃをユーザ情報ＤＢ１１３に仮登録するよう利用権管理装置１１ｂに要求するための情報である。ステップＳ４２を具体的に説明すると、まず、仮登録要求生成部２２３は、機器識別子格納部２１１から機器識別子Ｉｄａを取り出した後、取り出した機器識別子Ｉｄａを登録済識別子Ｉｄａとして扱う。そして、仮登録要求生成部２２３は、登録済識別子Ｉｄａおよび登録対象識別子Ｉｄｃの組み合わせに、予め保持する仮登録要求識別子Ｉｐｒｓを付加して、仮登録要求Ｄｐｒｓｃ（図２６（ａ）参照）を生成する。ここで、仮登録要求識別子Ｉｐｒｓは、利用権管理装置１１ｂが仮登録要求Ｄｐｒｓｃを特定するために使用される。仮登録要求生成部２２３は、以上の仮登録要求Ｄｐｒｓｃを通信部２１３に渡す。通信部２１３は、受け取った仮登録要求Ｄｐｒｓｃを、伝送路３１を通じて、利用権管理装置１１ｂに送信する。

【０１０９】利用権管理装置１１ｂ（図２１参照）において、通信部１１５は、伝送路３１からの受信情報に仮登録要求識別子Ｉｐｒｓが含まれていることから、仮登録要求Ｄｐｒｓｃを今回受信したことを認識する。この認識結果に従って、通信部１１５は、受信仮登録要求Ｄｐｒｓｃを、ユーザ情報管理部１２６に渡す。ユーザ情報管理部１２６は、受信仮登録要求Ｄｐｒｓｃから登録済識別子Ｉｄａを取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子Ｉｄａを含む契約者レコードＲｃｓ（図７（ａ）参照）を検索する（ステップＳ４３）。その後、ユーザ情報管理部１２６は、図１８のステップＳ３３およびＳ３４と同様の処理を行って（ステップＳ４４，Ｓ４５）、ステップＳ４５において、機器識別子数Ｎｄｖが上限値Ｖｕｌ未満でないと判断した場合には、図１８のステップＳ３９と同様の処理を行う（ステップＳ４６）。この場合、機器２１ａは、図１８のステップＳ３１０と同様の処理を行う（ステップＳ４７）。

【０１１０】それに対して、ステップＳ４５において、機器識別子数Ｎｄｖが上限値Ｖｕｌ未満であると判断した場合に、受信仮登録要求Ｄｐｒｓｃから登録対象識別子Ｉｄｃを取り出した後、取り出したものと、それが仮登録された機器識別子Ｉｄｃであることを示す仮登録フラグＦｐｓとを、対象となる契約者レコードＲｃｓに追加する（ステップＳ４８）。契約者レコードＲｃｓは、図７（ａ）に示すものから、図２７（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１２６は、登録対象識別子Ｉｄｃの仮登録が完了した旨を登録完了生成部１２７に通知し、さらに、受信仮登録要求Ｄｐｒｓｃ内の登録済識別子Ｉｄａを登録完了生成部１２７に渡す。

【０１１１】登録完了生成部１２７は、ユーザ情報管理部１２６から仮登録が完了したことが通知されると、図２６（ｂ）に示す仮登録完了通知Ｄpsccを生成し、機器２１ａに送信する（ステップＳ４９）。仮登録完了通知Ｄpsccは、登録対象識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に仮登録したことを機器２１ａに通知するための情報である。ステップＳ４８をより具体的に説明すると、まず、登録完了生成部１２７は、ユーザ情報管理部１２６から受け取った登録済識別子ＩｄｖａにＩｐｓｃを付加して、仮登録完了通知Ｄpscc（図２６（ｂ）参照）を生成する。ここで、仮登録完了識別子Ｉｐｓｃは、機器２１ａが仮登録完了通知Ｄpsccを特定するために使用される。以上の仮登録完了通知Ｄpsccは、登録完了生成部１２７から、通信部１１５および伝送路３１を通じて、機器２１ａに送信される。

【０１１２】機器２１ａ（図２２参照）において、通信部２１３は、伝送路３１からの受信情報に含まれる仮登録完了識別子ＩｐｓｃおよびＩｄｖａから、今回の受信情報が自分宛の仮登録完了通知Ｄpsccであることを認識する。この認識結果に従って、通信部２１３は、受信仮登録完了通知Ｄpsccを、仮登録完了出力部２２４に渡す。仮登録完了出力部２２４は、受信仮登録完了Ｄpsccに応答して、機器識別子ＩｄｖｃのＩｄｖａが仮登録が完了したことを、画像または音声で出力し（ステップＳ４１０）、そのことをユーザβに伝える。これによって、機器２１ａ側の処理が終了する。

【０１１３】仮登録完了を認識すると、ユーザβは、機器２１ｃを操作して、機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に本登録する旨を指定する。この指定に関連して、機器２１ｃの機器識別子入力部２２５は、ユーザβが機器２１ｃを操作することにより入力された機器２１ａの機器識別子（登録済識別子）Ｉｄｖａを、本登録要求生成部２２６に通知する（図２５；ステップＳ５１）。この通知に応答して、本登録要求生成部２２６は、図２８（ａ）に示す本登録要求Ｄcrscを生成し、利用権管理装置１１ｂに送信する（ステップＳ５２）。本登録要求Ｄcrscは、機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に本登録するよう利用権管理装置１１ｂに要求するための情報である。ステップＳ５２をより具体的に説明すると、まず、本登録要求生成部２２６は、機器識別子格納部２１１から機器識別子（つまり、登録対象識別子）Ｉｄｖｃを取り出した後、取り出した登録対象識別子Ｉｄｖｃと、通知された登録済識別子Ｉｄｖａとの組み合わせに、予め保持する本登録要求識別子Ｉｃｒｓを付加して、本登録要求Ｄcrsc（図２８（ａ）参照）を生成する。ここで、本登録要求識別子Ｉｃｒｓは、利用権管理装置１１ｂが本登録要求Ｄcrscを特定するために使用される。本登録要求生成部２２６は、以上の本登録要求Ｄcrscを、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｂに送信する。

【０１１４】利用権管理装置１１ｂ（図２１参照）において、通信部１１５は、伝送路３１からの受信情報に含まれる本登録要求識別子ＩｃｒｓからＣｒｓを、今回の受信情報が本登録要求Ｄcrscであることを認識する。この認識結果に従って、受信本登録要求Ｄcrscはユーザ情報管理部１２６に渡され、ユーザ情報管理部１２６は、受信本登録要求Ｄcrscから、機器識別子ＩｄｖａおよびＩｄｖｃの双方を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した両機器識別子ＩｄｖａおよびＩｄｖｅを含む契約者レコードＲｃｓ（図２７（ａ）参照）を検索する（ステップＳ５３）。その後、ユーザ情報管理部１２６は、検索した契約者レコードＲｃｓから、仮登録フラグＦｐｓを削除し（ステップＳ５４）、さらに、それに含まれる機器識別子数Ｎｄｖを１だけインクリメントする（ステップＳ５５）。これによって、機器識別子Ｉｄｖｃの本登録が完了し、その結果、契約者レコードＲｃｓは、図２７（ａ）に示すものから、同図（ｂ）に示すようなものに更新される。その後、ユーザ情報管理部１２６は、登録対象識別子Ｉｄｖｃの本登録が完了した旨を登録完了生成部１２７に通知し、さらに、受信本登録要求Ｄcrsc内の登録対象識別子Ｉｄｖｃを登録完了生成部１２７に渡す。

【０１１５】登録完了生成部１２７は、ユーザ情報管理部１２６から本登録が完了したことが通知されると、図２８（ｂ）に示す本登録完了通知Ｄcsccを生成し、機器２１ｃに送信する（ステップＳ５６）。本登録完了通知Ｄcsccは、ユーザ情報ＤＢ１１３に機器識別子Ｉｄｖｃの本登録が完了したことを機器２１ｃに通知するための情報である。ステップＳ５６をより具体的に説明すると、まず、登録完了生成部１２７は、ユーザ情報管理部１２６から受け取った登録対象識別子Ｉｄｖｃを登録済識別子Ｉｄｖｃとして扱い、これに、予め保持する本登録完了識別子Ｉｃｓｃを付加して、本登録完了通知Ｄcscc（図２８（ｂ）参照）を生成する。ここで、本登録完了識別子Ｉｃｓｃは、機器２１ｃが本登録完了通知Ｄcsccを特定するために使用される。以上の本登録完了通知Ｄcsccは、通信部２１３および伝送路３１を通じて、機器２１ｃに送信される。

【０１１６】機器２１ｃ（図２３参照）において、通信部２１３は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる本登録完了識別子Ｉｃｓｃおよび登録対象識別子Ｉｄｖｃから、今回の受信情報が自分宛の本登録完了通知Ｄcsccであることを認識する。この認識結果に従って、通信部２１３は、受信本登録完了通知Ｄcsccを、設定要求生成部２１２に渡す。設定要求生成部２１２は、受信情報に設定されている本登録完了識別子Ｉｃｓｃから、今回本登録完了通知Ｄcsccを受信したことを認識する（ステップＳ５７）。この認識結果に従って、設定要求生成部２１２は図８のステップＳ１１を実行可能な状態になったと判断し、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様に、利用

権管理装置１１ｂとデータ通信を行う。

【０１１７】前述の第１の変型例に係る機器識別子Ｉｄｖｃの追加登録では、利用権管理装置１１ａは、機器２１ｃが本当にユーザβにより所有されているか否かを判断できないまま、機器識別子Ｉｄｖｃを、ユーザβの契約者レコードＲｃｓに登録していた。しかしながら、本変型例では、仮登録の時に機器２１ａが送信する仮登録要求ＤｐｒｓｃＩに、登録済識別子Ｉｄｖａと、登録対象識別子Ｉｄｖｃとが設定され、本登録の時に機器２１ｃが送信する本登録要求ＤｃｒｓｃＩに、登録済識別子Ｉｄｖａと、登録対象識別子Ｉｄｖｃとが設定されることにより、機器２１ａおよび２１ｃの間に関連性があることを証明することが可能となる。これによって、利用権管理装置１１ｂは、機器２１ｃが機器２１ａのユーザβにより所有されていると判断できる。このように、本変型例では、ユーザβの所有物でない機器２１がユーザβの契約者レコードＲｃｓに登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システムＳａ２を提供できるようになる。

【０１１８】なお、以上の変型例では、機器２１ｃの機器識別子Ｉｄｖｃの追加登録のために、機器２１ａが動作する例について説明した。しかし、これに限らず、機器２１ｂも機器２１ａと同様に動作することで、機器識別子Ｉｄｖｃの追加登録に関与できるようになる。

【０１１９】「第３の変型例」次に、第３の変型例に係る利用権管理装置１１ｃを収容したライセンス情報管理システムＳａ３の全体構成について説明する。ライセンス情報管理システムＳａ３は、図１のライセンス情報管理システムＳａと比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｃを備えている点と、機器２１ｃをさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ３に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１２０】利用権管理装置１１ｃは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図２９に示すように、ユーザ情報管理部１２８と、パスワード通知生成部１２９と、登録完了生成部１３０とをさらに備える点で相違する。それ以外に両利用権管理装置１１およびＩＩｃの間に相違点は無い。それ故、図２９において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１２１】機器２１ａまたは機器２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉｄｖａおよびｄｖｂは、利用権管理装置１１ｃのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａまたは２１ｂは、機器２１ｃの機器識別子Ｉｄｖｃの登録のために、図４と比較すると、図３０に示すように、パスワード入力部２２７と、登録要求生成部２２８と、登録完了出力部２２９とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａおよび２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図３０において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１２２】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ｃのユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１ａまたは２１ｂと比較すると、図３１に示すように、機器識別子入力部２３０、パスワード要求生成部２３１およびパスワード通知部２３２をさらに備える点で相違する。それ以外に、両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図３１において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１２３】次に、図３２および図３３を参照して、以上のような構成のライセンス情報管理システムＳａ３において、機器２１ｃの機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｃの動作について説明する。ユーザβは、機器２１ｃを操作して、機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に仮登録する旨を指定する。この指定に関連して、機器２１ｃの機器識別子入力部２３０は、ユーザβが機器２１ｃを操作することにより入力された機器２１ａの機器識別子（以下、登録済識別子と称する）Ｉｄｖａを、パスワード要求生成部２３１に通知する（図３２；ステップＳ６１）。パスワード要求生成部２３１は、上述の通知に応答して、図３４（ａ）に示すパスワード要求Ｄｒｐｓを生成し、利用権管理装置１１ｃに送信する（ステップＳ６２）。パスワード要求Ｄｒｐｓは、登録対象識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に登録するために必要となるパスワードＷｐｓｓの発行を利用権管理装置１１ｃに要求するための情報である。ステップＳ６２を具体的に説明すると、まず、パスワード要求生成部２３１は、機器識別子格納部２１１から登録対象識別子Ｉｄｖｃを取り出した後、取り出した登録対象識別子Ｉｄｖｃと、通知された登録済識別子Ｉｄｖａとで構成される組みに、予め保持するパスワード要求識別子Ｉｒｐｓを付加して、パスワード要求Ｄｒｐｓ（図３４（ａ）参照）を生成する。ここで、パスワード要求識別子Ｉｒｐｓは、利用権管理装置１１ｃがパスワード要求Ｄｒｐｓを特定するために使用される。パスワード要求生成部２３１は、以上のパスワード要求Ｄｒｐｓを、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｃの通信部１１５に送信する。

【０１２４】利用権管理装置１１ｃ（図２９参照）において、通信部１１５は、受信情報内のパスワード要求識別子Ｉｒｐｓから、パスワード要求Ｄｒｐｓを今回受信したことを認識する。この認識結果に従って、通信部１１５は、受信パスワード要求Ｄｒｐｓを、ユーザ情報管理部１

２８に渡す。ユーザ情報管理部１２８は、受信パスワード要求Drps から登録済識別子 Idva を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子 Idva を含む契約者レコードRcs（図７（ａ）参照）を検索する（ステップＳ６３）。その後、ユーザ情報管理部１２８は、図１８のステップＳ３３およびＳ３４と同様の処理を行って（ステップＳ６４，Ｓ６５）、ステップＳ６５において、機器識別子数Ndvが上限値Vul以上であると判断した場合には、図１８のステップＳ３９と同様の処理を行う（ステップＳ６６）。この場合、機器２１ｃは、図１８のステップＳ３１０と同様の処理を行う（ステップＳ６７）。

【０１２５】それに対して、ステップＳ６５において、機器識別子数Ndvが上限値Vul以上でないと判断した場合に、ユーザ情報管理部１２８は、ステップＳ６８を行い、まず、上述のパスワードWpss を生成する。パスワードWpss は、典型的には、ユーザ情報管理部１２８が無作為に選んだ文字または記号の組み合わせであることが好ましい。さらに、ユーザ情報管理部１２８は、受信パスワード要求Drpsから登録対象識別子 Idvc を取り出した後、取り出したものと、生成したパスワードWpss とを、ステップＳ６３で検索した契約者レコードRcs に追加して、登録対象識別子 Idvc の仮登録を行う（ステップＳ６８）。これによって、契約者レコードRcs は、図７（ａ）に示すものから、図３５（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１２８は、登録対象識別子 Idvc の仮登録が完了した旨をパスワード通知生成部１２９に通知し、さらに、受信パスワード要求Drps 内の登録対象識別子 Idvc およびステップＳ６８で生成したパスワードWpss を、パスワード通知生成部１２９に渡す。

【０１２６】パスワード通知生成部１２９は、ユーザ情報管理部１２８から仮登録が完了したことが通知されると、図３４（ｂ）に示すパスワード通知Dpss を生成し、機器２１ｃに送信する（ステップＳ６９）。パスワード通知Dpss は、登録対象識別子 Idvc の登録のために生成したパスワードWpss を機器２１ｃに通知するための情報である。ステップＳ６９をより具体的に説明すると、まず、パスワード通知生成部１２９は、ユーザ情報管理部１２６から受け取った登録対象識別子 Idvc およびパスワードWpss の組み合わせに、予め保持するパスワード通知識別子 Ipss を付加して、パスワード通知Dpss （図３４（ｂ）参照）を生成する。ここで、パスワード通知識別子 Ipss は、機器２１ｃがパスワード通知Dpss を特定するために使用される。以上のパスワード通知Dpss は、パスワード通知生成部１２９から、通信部１１５および伝送路３１を通じて、機器２１ｃの通信部２１３に送信される。

【０１２７】機器２１ｃ（図３１参照）において、通信部２１３は、受信信号内のパスワード通知識別子 Ipss および登録対象識別子 Idvc から、今回の受信情報が自分宛のパスワード通知Dpss であることを認識する。この認識結果に従って、通信部２１３は、受信パスワード通知Dpss を、パスワード通知部２３２に渡す。パスワード通知部２３２は、パスワード通知Dpss に含まれるパスワードWpss を画像出力または音声出力することで、それをユーザβに通知する（ステップＳ６１０）。これによって、機器２１ｃ側の処理が終了する。なお、ステップＳ６１０において、パスワード通知部２３２は、パスワードWpss の通知に加えて、登録対象識別子 Idvc の仮登録が終了したことを画像または音声でユーザβに伝えても良い。

【０１２８】仮登録完了を認識すると、ユーザβは、機器２１ａを操作して、機器識別子 Idvc をユーザ情報ＤＢ１１３にて本登録する旨を指定する。この指定に関連して、機器２１ａのパスワード入力部２２７は、ユーザβが機器２１ａを操作することにより入力されたパスワードWpss を、登録要求生成部２２８に通知する（図３３；ステップＳ７１）。この通知に応答して、登録要求生成部２２８は、図３６（ａ）に示す登録要求Drsc を生成し、利用権管理装置１１ｃに送信する（ステップＳ７２）。登録要求Drsc は、登録対象識別子 Idvc をユーザ情報ＤＢ１１３にて本登録するよう利用権管理装置１１ｃに要求するための情報である。ステップＳ７２を具体的に説明すると、まず、登録要求生成部２２８は、機器識別子格納部２１１から機器識別子（つまり、登録済識別子） Idva を取り出した後、取り出したものと、通知されたパスワードWpss との組み、予め保持する登録要求識別子 Irsを付加して、登録要求Drsc （図３６（ａ）参照）を生成する。ここで、登録要求識別子 Irs は、利用権管理装置１１ｃが登録要求Drsc を特定するために使用される。登録要求生成部２２８は、以上の登録要求Drsc を、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｃに送信する。

【０１２９】利用権管理装置１１ｃ（図２９参照）において、通信部１１５は、受信情報に含まれる登録要求識別子 Irsから、今回の受信情報が登録要求Drsc であることを認識する。この認識結果に従って、受信登録要求Drsc はユーザ情報管理部１２８に渡され、ユーザ情報管理部１２８は、受信登録要求Drsc から、登録済識別子 Idva およびパスワードWpss の双方を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子 Idva およびパスワードWpss を含む契約者レコードRcs（図３５（ａ）参照）を検索する（ステップＳ７３）。その後、ユーザ情報管理部１２８は、検索した契約者レコードRcsから、パスワードWpss を削除し（ステップＳ７４）、さらに、それに含まれる機器識別子数Ndvを１だけインクリメントする（ステップＳ７５）。これによって、機器識別子 Idvc の本登録が完了し、その結果、契約者レコードRcsは、図３５（ａ）

に示すものから、同図（ｂ）に示すようなものに更新される。その後、ユーザ情報管理部１２８は、登録対象識別子Ｉｄｖｃ の本登録が完了した旨を登録完了生成部１３０に通知し、さらに、受信登録要求Ｄｒｓｃ 内の登録済識別子Ｉｄｖａ を登録完了生成部１３０に渡す。

【０１３０】登録完了生成部１３０は、ユーザ情報管理部１２８から本登録が完了したことが通知されると、図３６（ｂ）に示す登録完了通知Ｄｓｃｃ を生成し、機器２１ａに送信する（ステップＳ７６）。登録完了通知Ｄｓｃｃ は、ユーザ情報ＤＢ１１３に機器識別子Ｉｄｖｃ の本登録が完了したことを機器２１ａ に通知するための情報である。ステップＳ７６をより具体的に説明すると、まず、登録完了生成部１３０は、ユーザ情報管理部１２８から受け取った登録済識別子Ｉｄｖａ に、予め保持する登録完了識別子Ｉｓｃを付加して、登録完了通知Ｄｓｃｃ （図３６（ｂ）参照）を生成する。ここで、登録完了識別子Ｉｓｃは、機器２１ａ が本登録完了通知Ｄｓｃｃ を特定するために使用される。以上の登録完了通知Ｄｓｃｃ は、通信部１１５および伝送路３１を通じて、機器２１ａ の通信部２１３に送信される。

【０１３１】機器２１ａ （図３０参照）において、通信部２１３は、受信情報に含まれる登録完了識別子Ｉｓｃおよび登録済識別子Ｉｄｖａ から、今回の受信情報が自分宛の登録完了通知Ｄｓｃｃ であることを認識する。この認識結果に従って、通信部２１３は、受信本登録完了通知Ｄｓｃｃ を、登録完了出力部２２９に渡す。登録完了出力部２２９は、受信情報内の登録完了識別子Ｉｓｃから、今回登録完了通知Ｄｓｃｃ を受信したことを認識し、登録対象識別子Ｉｄｖｃ の本登録が完了したことを画像出力または音声出力して（ステップＳ７７）、ユーザβにその旨を伝える。これによって、機器２１ｃ は、図８のステップＳ１１を実行可能な状態になる。そして、機器２１ｃ は、必要に応じて、以降は第１の実施形態で説明した機器２１ａ または機器２１ｂ と同様の処理を行って、コンテンツデータＤｃｎｔ を利用する。

【０１３２】上述の第３の変型例によれば、利用権管理装置１１ｃ のユーザ情報ＤＢ１１３に登録済みの機器２１ａ が、未登録の機器２１ｃ の機器識別子Ｉｄｖｃ の登録に関与することで、第２の変型例と同様に、ユーザβの所有物でない機器２１ｃ がユーザβの契約者レコードＲｃｓに登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システムＳａ３を提供できるようになる。

【０１３３】なお、以上の変型例では、機器２１ｃ の機器識別子Ｉｄｖｃ の追加登録のために、機器２１ａ が動作する例について説明した。しかし、これに限らず、機器２１ｂ も機器２１ａ と同様に動作することで、機器識別子Ｉｄｖｃ の追加登録に関与できるようになる。

【０１３４】「第４の変型例」次に、第４の変型例に係る利用権管理装置１１ｄ を収容したライセンス情報管理システムＳａ４の全体構成について説明する。ライセンス情報管理システムＳａ４は、図１のライセンス情報管理システムＳａ と比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｄ を備えている点と、機器２１ｃ をさらに備えている点と、機器２１ａ および２１ｃ が通信ケーブル３２を介して通信可能に接続される点とで相違する。それ以外に両ライセンス情報管理システムＳａ およびＳａ４に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１３５】利用権管理装置１１ｄ は、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図３７に示すように、ユーザ情報管理部１３１と、登録完了生成部１３２とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｄ の間に相違点は無い。それ故、図３７において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１３６】機器２１ａ または２１ｂ は、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉｄｖａ およびＩｄｖｂ は、利用権管理装置１１ｄ のユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａ または２１ｂ は、機器２１ｃ の機器識別子Ｉｄｖｃ の登録のために、図４と比較すると、図３８に示すように、通信部２２８と、登録要求生成部２２９と、登録完了通知部２３０とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａ および２１ｂ と、第１の実施形態に係るものとの間に相違点は無い。それ故、図３８において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１３７】機器２１ｃ は、上述のユーザβにより所有されるが、現時点では、自身に割り当てられた機器識別子Ｉｄｖｃ が利用権管理装置１１ｄ のユーザ情報ＤＢ１１３に未登録であって、図４の機器２１ａ または２１ｂ と比較すると、図３９に示すように、登録要求生成部２３１と、通信部２３２とをさらに備える点で相違する。それ以外に、図４の両機器２１ａ および２１ｂ と、機器２１ｃ との間には相違点は無い。それ故、図３９において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１３８】次に、図４０を参照して、以上のような構成のライセンス情報管理システムＳａ４において、機器２１ｃ の機器識別子Ｉｄｖｃ をユーザ情報ＤＢ１１３に登録するまでの機器２１ａ 、機器２１ｃ および利用権管理装置１１ｄ の動作について説明する。ユーザβは、機器２１ｃ を操作して、機器識別子Ｉｄｖｃ をユーザ情報ＤＢ１１３に登録する旨を指定する。この指定に応答して、機器２１ｃ の登録要求生成部２３１は、図４１（ａ）に示す第１の登録要求Ｄｒｓｃ１を生成し、通信ケーブル３２を通じて、機器２１ａ に送信する（図４０；ステップＳ８

１）。第１の登録要求Ｄrsc1は、登録対象識別子ＩdvcをユーザＤＢ１１３に登録することを、機器２１cの代わりに機器２１aに要求するための情報である。ステップＳ８１を具体的に説明すると、まず、登録要求生成部２３１は、機器識別子格納部２１１から機器識別子（以下、登録対象識別子と称する）Ｉdvcを取り出した後、取り出した登録対象識別子Ｉdvcに、予め保持する第１の登録要求識別子Ｉrs1を付加して、第１の登録要求Ｄrsc1（図４１（ａ）参照）を生成する。ここで、第１の登録要求識別子Ｉrs1は、機器２１aが第１の登録要求Ｄrsc1を特定するために使用される。登録要求生成部２３１は、以上の第１の登録要求Ｄrsc1を、通信部２３２および通信ケーブル３２を通じて、機器２１aに送信する。

【０１３９】機器２１a（図３８参照）において、通信部２２８は、受信情報内の第１の登録要求識別子Ｉrs1から、第１の登録要求Ｄrsc1を今回受信したことを認識する（ステップＳ８２）。この認識結果に従って、通信部２２８は、受信した第１の登録要求Ｄrsc1を、登録要求生成部２２９に渡す。それに応答して、登録要求生成部２２９は、図４１（ｂ）に示す第２の登録要求Ｄrsc2を生成し、伝送路３１を通じて、利用権管理装置１１dに送信する（ステップＳ８３）。第２の登録要求Ｄrsc2は、登録対象識別子Ｉdvcをユーザ情報ＤＢ１１３に登録することを、利用権管理装置１１dに要求するための情報である。ステップＳ８３を具体的に説明すると、まず、登録要求生成部２２９は、機器識別子格納部２１１から機器識別子（以下、登録済識別子と称する）Ｉdvaを取り出した後、取り出した登録済識別子Ｉdvaを、今回受信した第１の登録要求Ｄrsc1に付加して、第２の登録要求Ｄrsc2（図４１（ｂ）参照）を生成する。ここで、第２の登録要求Ｄrsc2において、第１の登録要求識別子Ｉrs1は、利用権管理装置１１dが第２の登録要求Ｄrsc2を特定するために使用される。登録要求生成部２２９は、以上の第２の登録要求Ｄrsc2を、通信部２１３および伝送路３１を通じて、利用権管理装置１１d（図３７参照）に送信する。

【０１４０】利用権管理装置１１dにおいて、通信部１１５は、伝送路３１からの受信情報内の第１の登録要求識別子Ｉrs1から、第２の登録要求Ｄrsc2を今回受信したことを認識する。その認識結果に従って、通信部１１５は、受信した第２の登録要求Ｄrsc2をユーザ情報管理部１３１に渡す。それに応答して、ユーザ情報管理部１３１は、受信した第２の登録要求Ｄrsc2から登録済識別子Ｉdvaを取り出し、ユーザ情報ＤＢ１１３にアクセスした後、図３２のステップＳ６３～Ｓ６５と同様の処理を行う（ステップＳ８４～Ｓ８６）。ユーザ情報管理部１３１は、ステップＳ８６において、機器識別子数Ndvが上限値Vul以上でないと判断した場合には、受信した第２の登録要求Ｄrsc2から登録対象識別子Ｉdvcを取り出した後、取り出したものを、ステップＳ８４で検索した契約者レコードＲcsに追加して、登録対象識別子Ｉdvcの登録を行う（ステップＳ８７）。これによって、契約者レコードＲcsは、図７（ａ）に示すものから、図３５（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１３１は、登録対象識別子Ｉdvcの登録が完了した旨を登録完了生成部１３２に通知し、さらに、受信した第２の登録要求Ｄrsc2内の登録済識別子Ｉdvaを、登録完了生成部１３２に渡す。

【０１４１】登録完了生成部１３２は、ユーザ情報管理部１３１から登録完了が通知されると、図４１（ｃ）に示す登録完了通知Ｄscc を生成し、機器２１aに送信する（ステップＳ８８）。登録完了通知Ｄscc は、登録対象識別子Ｉdvcのユーザ情報ＤＢ１１３への登録が完了したことを機器２１aに通知するための情報である。ステップＳ８８をより具体的に説明すると、まず、登録完了生成部１３２は、ユーザ情報管理部１３１から受け取った登録済識別子Ｉdvaに、予め保持する登録完了識別子Ｉscを付加して、登録完了通知Ｄscc （図４１（ｃ）参照）を生成する。ここで、登録完了識別子Ｉscは、機器２１aが登録完了通知Ｄscc を特定するために使用される。以上の登録完了通知Ｄscc は、登録完了生成部１３２から、通信部１１５および伝送路３１を通じて、機器２１aの通信部２１３に送信される。

【０１４２】機器２１a（図３８参照）において、通信部２１３は、受信信号内の登録完了識別子Ｉsc および登録済識別子Ｉdvaから、今回の受信情報が自分宛の登録完了通知Ｄscc であることを認識する。この認識結果に従って、通信部２１３は、受信登録完了通知Ｄscc を、登録完了通知部２３０に渡す。それに応じて、登録完了通知２３０は、登録対象識別子Ｉdvcの登録が完了したことを画像出力または音声出力することで、それをユーザβに通知する（ステップＳ６１０）。これによって、ユーザβは、機器２１cの機器識別子Ｉdvcが登録されたことを認識し、機器２１cは、図８のステップＳ１１を実行可能な状態になる。そして、機器２１cは、必要に応じて、以降は第１の実施形態で説明した機器２１aまたは機器２１bと同様の処理を行って、コンテンツデータＤcnt を利用する。

【０１４３】また、ステップＳ８６において、機器識別子数Ndvが上限値Vul以上であると判断された場合、従前の実施形態と同様に、利用権管理装置１１dから機器２１aに、登録拒否通知Ｄrsc が送信される（ステップＳ８１０，Ｓ８１１）。

【０１４４】上述の第４の変型例によれば、利用権管理装置１１dのユーザ情報ＤＢ１１３に登録済みの機器２１aが、未登録の機器２１cの機器識別子Ｉdvcの登録に関与することで、第２の変型例と同様に、ユーザβの所有物でない機器２１がユーザβの契約者レコードＲcsに登録されにくい、機器識別子の追加登録を行えるライ

センス情報管理システムＳａ4を提供できるようになる。さらに、本変型例では、図３２および図３３の組み合わせと、図４０とを比較すれば分かるように、機器２１ａおよび２１ｃをケーブル３２で通信可能に接続することで、機器識別子Ｉｄｖｃの登録までに必要な処理を減らすことができる。

【０１４５】なお、以上の変型例では、機器２１ｃの機器識別子Ｉｄｖｃの追加登録のために、機器２１ａが動作する例について説明した。しかし、これに限らず、機器２１ｂも機器２１ａと同様に動作することで、機器識別子Ｉｄｖｃの追加登録に関与できるようになる。

【０１４６】また、以上の変型例では、機器２１ａおよび機器２１ｃを通信可能に接続するために通信ケーブル３２を用いたが、これに限らず、機器２１ａおよび２１ｃは無線通信を行っても良い。他にも、機器２１ａおよび２１ｃは伝送路３１を介して通信を行っても良い。

【０１４７】また、以上の変型例では、登録完了通知Ｄｓｃｃは、利用権管理装置１１ｄから機器２１ａに送信されていた。しかし、これに限らず、利用権管理装置１１ｄから機器２１ｃに送信されても良い。また、機器２１ａに送信された登録完了通知Ｄｓｃｃは機器２１ｃに転送されても良い。この場合、登録完了したことは、機器２１ｃから音声または画像によりユーザβに通知される。

【０１４８】また、以上の第２～第４の変型例では、単一の機器２１ｃの機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に追加登録するための処理について説明したが、２台以上の機器２１の機器識別子Ｉｄｖを追加する場合にも、第２～第４の変型例を容易に応用することができる。

【０１４９】また、以上の第２～第４の変型例では、機器識別子Ｉｄｖｃの追加登録に関与できるのは、機器２１ａでも、機器２１ｂでも良いと説明した。しかし、これに限らず、機器２１ａおよび２１ｂのいずれか一方に、機器識別子Ｉｄｖの追加登録に関与できる権限を与え、権限を持つ機器２１のみが機器識別子Ｉｄｖの追加登録に関与できるようにしても良い。

【０１５０】また、以上の第１～第４の変型例において、ユーザ情報ＤＢ１１３には、図７（ａ）に示す情報の他に、ユーザβに関連するユーザ情報をさらに登録しておき、機器２１ａまたは２１ｃは、利用権管理装置１１ａ～１１ｄにアクセスする際に、ユーザβにより入力されたユーザ情報を送信する。利用権管理装置１１ａ～１１ｄは、受信ユーザ情報を、予め格納されているユーザ情報と照合することで、機器２１ｃが機器２１ａと同じユーザβにより所有されているか否かを判断するようにしても良い。

【０１５１】また、第１の実施形態では、ユーザ情報ＤＢ１１３に契約時に登録された機器２１ａおよび２１ｂが同一の利用権情報Ｄｒｇｔを共有する例について説明した。しかし、ユーザβは、ユーザ情報ＤＢ１１３または利用権ＤＢ１１４から、既に登録されている機器２１ｂの機器識別子Ｉｄｖｂを削除したい場合がある。以下に説明する利用権管理装置１１ｅは、上述の利用権管理装置１１の第５の変型例であって、上述のニーズに対応するために提供される。

【０１５２】「第５の変型例」図４２は、利用権管理装置１１ｅを収容したライセンス情報管理システムＳａ5の全体構成を示すブロック図である。ライセンス情報管理システムＳａ5は、図１のライセンス情報管理システムＳａと比較すると、利用権管理装置１１が利用権管理装置１１ｅに代わる点でのみ相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ5には相違点は無い。それ故、図４２において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１５３】利用権管理装置１１ｅは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図４３に示すように、機器識別子削除部１３３および削除完了作成部１３４をさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｅの間に相違点は無い。それ故、図４３において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１５４】機器２１ａまたは２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉｄｖａおよびｄｖｂは、利用権管理装置１１ｅのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。さらに、機器２１ａおよび２１ｂは、利用権管理装置１１ｅの利用権ＤＢ１１４に登録されている利用権レコードＲｒｇｔを共有している（図７（ｂ）参照）。また、機器２１ｂは、機器識別子Ｉｄｖｂの削除のために、図４と比較すると、図４４に示すように、削除要求生成部２３３と、削除完了通知部２３４とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図４４において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１５５】次に、図４５を参照して、以上のような構成のライセンス情報管理システムＳａ5において、機器２１ｂの機器識別子Ｉｄｖｂをユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するまでの機器２１ｂおよび利用権管理装置１１ｅの動作について説明する。ユーザβは、機器２１ｂを操作して、機器識別子Ｉｄｖｂをユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除する旨を指定する。この指定に応答して、機器２１ｂにおいて、削除要求生成部２３３は、図４６（ａ）に示す削除要求Ｄｒｗｂを生成し、利用権管理装置１１ｅに送信する（図４５；ステップＳ９１）。削除要求Ｄｒｗｂは、本機器２１ｂをユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するよう利用権管理装置１１ｅに要求するた

めの情報である。ステップＳ９１をより具体的に説明すると、まず、削除要求生成部２３３は、機器識別子格納部２１１から機器識別子Ｉｄｖｂを取り出した後、取り出したものを削除対象識別子Ｉｄｖｂとして、予め保持する削除要求識別子ＩｒｗをＩＤ付加して、削除要求Ｄｒｗｂ（図４６（ａ）参照）を生成する。ここで、削除要求識別子ＩｒｗＩＤは、利用権管理装置１１ｅが削除要求Ｄｒｗｂを特定するために使用される。以上の削除要求Ｄｒｗｂは、削除要求生成部２３３から、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｅに送信される。

【０１５６】利用権管理装置１１ｅ（図４３参照）において、通信部１１５は、伝送路３１からの受信情報に含まれる削除要求識別子Ｉｒｗから、今回の受信情報が削除要求Ｄｒｗｂであることを認識する。この認識結果に従って、通信部１１５は、受信削除要求Ｄｒｗｂを、機器識別子削除部１３３に渡す。機器識別子削除部１３３は、受信削除要求Ｄｒｗｂから削除対象識別子Ｉｄｖｂを取り出した後、ユーザ情報ＤＢ１１３内の契約者レコードＲｃｓ（図７（ａ）参照）から、取り出した削除対象識別子Ｉｄｖｂを検索して削除する（ステップＳ９２）。さらに、機器識別子削除部１３３は、ステップＳ９２で検索した契約者レコードＲｃｓに含まれる機器識別子数Ｎｄｖを１だけデクリメントする（ステップＳ９３）。その結果、契約者レコードＲｃｓは、図７（ａ）に示すものから、図４７（ａ）に示すようなものに更新される。

【０１５７】さらに、機器識別子削除部１３３は、利用権ＤＢ１１４内の利用権レコードＲｒｇｔから、受信削除要求Ｉｒｗｂから取り出した削除対象識別子Ｉｄｖｂを検索して削除する（ステップＳ９４）。その結果、利用権レコードＲｒｇｔは、図７（ｂ）に示すものから、図４７（ｂ）に示すようなものに更新される。その後、機器識別子削除部１３３は、契約者レコードＲｃｓおよび利用権レコードＲｒｇｔを正しく更新した旨と、受信登録要求Ｄｒｓｃ内の削除対象識別子Ｉｄｖｂとを削除完了生成部１３４に通知する。

【０１５８】削除完了生成部１３４は、削除対象識別子Ｉｄｖｂの削除が完了したことが通知されると、図４６（ｂ）に示す削除完了通知Ｄｓｗｂを生成し、機器２１ｂに送信する（ステップＳ９５）。削除完了通知Ｄｓｗｂは、削除対象識別子Ｉｄｖｂを削除したことを機器２１ｂに通知するための情報である。ステップＳ９５をより具体的に説明すると、まず、削除完了生成部１３４は、受け取った削除対象識別子Ｉｄｖｂに、予め保持する削除完了識別子ＩｓｗをＩＤ付加して、削除完了通知Ｄｓｗｂ（図４６（ｂ）参照）を生成する。ここで、削除完了識別子Ｉｓｗは、機器２１ｂが削除完了通知Ｄｓｗｂを特定するために使用される。以上の削除完了通知Ｄｓｗｂは、通信部１１５および伝送路３１を通じて、機器２１ｂに送信される。

【０１５９】機器２１ｂ（図４３参照）において、通信部２１３は、伝送路３１からの受信情報に含まれる削除完了識別子Ｉｓｗから、今回の受信情報が削除完了通知Ｄｓｗｂであることを認識する。この認識結果に従って、通信部２１３は、受信削除完了通知Ｄｓｗｂを、削除完了通知部２３４に渡す。削除完了通知部２３４は、削除完了通知Ｄｓｗｂを受信し（ステップＳ９６）、その後、機器識別子Ｉｄｖｂが正常に削除されたことを、画像または音声で出力して、ユーザβにその旨を通知する。

【０１６０】以上のように本変型例によれば、利用権管理装置１１ｅおよび機器２１ｂのデータ通信により、ユーザβが不必要となった機器２１ｂの機器識別子Ｉｄｖｂを、ユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除することが可能になるので、より使い勝手の良いライセンス情報管理システムＳａ５を提供できるようになる。

【０１６１】なお、以上の変型例では、機器２１ｂ自身が、機器識別子Ｉｄｖｂの削除要求Ｄｒｗｂを生成して利用権管理装置１１ｅに送信するようにしたが、これに限らず、機器２１ａが、機器２１ｂの代わりに、削除要求Ｄｒｗｂを生成して、利用権管理装置１１ｅに送信するようにしても良い。さらに、機器２１ａおよび２１ｂのいずれかに削除要求Ｄｒｗｂを生成する権限を与え、権限が与えられた機器２１ａまたは２１ｂのみが削除要求Ｄｒｗｂを利用権管理装置１１ｅに送信可能にしても良い。

【０１６２】また、以上の変型例では、削除要求Ｄｒｗｂには、１個の削除対象識別子ＩｄｖｂがＩＤ設定されるように説明したが、これに限らず、複数の機器識別子Ｉｄｖｂが設定されても良い。さらに、削除要求Ｄｒｗｂが、第１の実施形態で説明したグループ識別子Ｉｇｐを含んでいる場合には、利用権管理装置１１ｅは、ユーザ情報ＤＢ１１３から、そのグループ識別子Ｉｇｐを含む契約者レコードＲｃｓを削除し、さらに、利用権ＤＢ１１４から、そのグループ識別子Ｉｇｐを含む利用権レコードＲｒｇｔの全てを削除するようにしても良い。

【０１６３】「第２の実施形態」図４８は、本発明の第２の実施形態に係る利用権管理装置４１を収容したライセンス情報管理システムＳｂの全体構成を示すブロック図である。図４８において、ライセンス情報管理システムＳｂは、利用権管理装置４１の他に、複数の機器５１の一例として２つの機器５１ａおよび５１ｂと、伝送路６１とを備えている。利用権管理装置４１は、コンテンツ配信に関わる事業者α側に設置される。また、機器５１ａおよび５１ｂは、典型的には、事業者αとの契約に基づいてコンテンツ配信を受ける契約者β(*)により使用される。また、伝送路６１は、有線または無線であり、利用権管理装置４１と、機器５１ａまたは機器５１ｂとをデータ通信可能に接続する。

【０１６４】次に、図４９を参照して、図４８の利用権管理装置４１の詳細な構成について説明する。図４９の利用権管理装置４１は、図２の利用権管理装置１１と比

較すると、利用権データベース１１４および利用権管理部１１７の代わりに、利用権データベース（以下、利用権ＤＢと称す）４１１および利用権管理部４１２を備えている点で相違する。それ以外に、両利用権管理装置１１および４１の間に構成面での相違点は無い。それ故、図４９において、図２の利用権管理装置１１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【０１６５】次に、図５０を参照して、図４８の機器５１ａおよび５１ｂの詳細な構成について説明する。図５０の機器５１ａおよび５１ｂは、図４の機器２１ａおよび２１ｂと比較して、設定要求生成部２１２の代わりに、設定要求生成部５１１を備えている点で相違する。それ以外に、機器５１ａおよび５１ｂと、機器２１ａおよび２１ｂとの間に構成面での相違点は無い。それ故、図５０において、図４の機器２１ａまたは２１ｂの構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【０１６６】次に、上記ライセンス情報管理システムＳｂにおいても、前述のライセンス情報管理システムＳａの場合と同様に、契約者βは事業者αからコンテンツ配信を受けるために必要となる準備を行う。この準備作業において、図６（ａ）、図６（ｂ）および図７（ａ）に示すコンテンツＤＢ１１１、復号鍵ＤＢ１１２およびユーザ情報ＤＢ１１３とが構築される。これらの詳細については、第１の実施形態で既に詳説しているので、本実施形態ではそれぞれの説明を省略する。

【０１６７】また、以上の準備作業において、事業者αは、機器５１ａおよび５１ｂに、それらを一意に特定するための機器識別子Ｉｄａおよび Ｉｄｂを割り当てる場合がある。以上の機器識別子Ｉｄａは、図５０に示す機器５１ａの機器識別子格納部２１１に設定され、機器識別子Ｉｄｂは、機器５１ｂの機器識別子格納部２１１に設定される。なお、機器識別子Ｉｄａおよび Ｉｄｂは、工場出荷時にそれぞれの機器識別子格納部２１１に設定されていても良い。

【０１６８】以上の準備が終了すると、機器５１ａおよび５１ｂの一方は、ユーザβの操作に従って、利用権管理装置４１から、コンテンツデータＤｃｎｔを取得することが可能となる。以下、図５１のフローチャートを参照して、コンテンツデータＤｃｎｔの取得時における機器５１ａおよび利用権管理装置４１の間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、コンテンツデータＤｃｎｔの取得時における機器５１ｂおよび利用権管理装置４１の間のデータ通信、およびそれに関連するそれぞれの動作については、機器５１ａのものと同様であるため、それぞれの説明を省略する。ここで、図５１は、図８と比較すると、ステップＳ１０１およびＳ１０３をさらに含む点と、ステップＳ１３の代わりにステップＳ１０２を含む点とで相違する。それ以外に両フローチャートに相違点は無いので、図５１において、図８のステップに相当するものには同一のステップ番号を付け、それぞれの説明を省略する。

【０１６９】ユーザβは、機器５１ａを操作して、利用権管理装置４１にアクセスし、コンテンツＤＢ１１１内のコンテンツデータＤｃｎｔから、今回取得したいもののコンテンツ識別子Ｉｃｎｔを指定する。以降の説明において、今回指定されたコンテンツデータＤｃｎｔを、取得対象コンテンツデータＤｃｎｔと称する。さらに、ユーザβは、取得対象コンテンツデータＤｃｎｔを利用する際の利用条件Ｃｃｎｔ（第１の実施形態参照）を指定する。

【０１７０】この指定に応答して、機器５１ａの設定要求生成部５１１は、今回指定されたものの中に共有対象識別子Ｉｄｖが含まれているか否かを判断する（ステップＳ１０１）。ここで、共有対象識別子Ｉｄｖとは、本ステップＳ１０１を実行する機器５１以外の他の機器５１の機器識別子Ｉｄでありて、共有対象となる利用権レコードＲｒｇｔａに登録済の機器５１の機器識別子Ｉｄである。上述から明らかなように、今回指定されるものには、共有対象識別子Ｉｄｖは含まれないので、設定要求生成部５１１は、図９（ａ）の同様の形式を有する第１の設定要求Ｄｒｒａ（第１の実施形態参照）を生成し、伝送路６１を通じて、利用権管理装置４１に送信する（ステップＳ１１）。本実施形態において、第１の設定要求Ｄｒｒａに含まれる設定要求識別子Ｉｒｒは、利用権管理装置４１が受信情報が第１の設定要求Ｄｒｒａおよび第２の設定要求Ｄｒｒ２ｂ のいずれかであることを特定するために使用される。

【０１７１】利用権管理装置４１（図４９参照）において、ユーザ認証部１１６は、伝送路６１からの第１の設定要求Ｄｒｒａの受信に応答して、認証処理を行い（ステップＳ１２）、その後、受け取った第１の設定要求Ｄｒｒａを利用権管理部４１２に渡す。利用権管理部４１２は、ユーザ認証部１１６からの受信情報内の設定要求識別子Ｉｒｒに基づいて、今回の受信情報が第１の設定要求Ｄｒｒａ または第２の設定要求Ｄｒｒ２ｂのいずれかであることを認識する。この認識結果に従って、利用権管理部４１２は、利用権データベース（以下、利用権ＤＢと称する）１１４への利用権登録処理を行う（ステップＳ１０２）。ステップＳ１０２において、より具体的には、利用権管理部４１２は、今回、第１の設定要求Ｄｒｒａを受信したか否かを判断する（ステップＳ１０２１）。ここで、ステップＳ１０２１では、受信情報が共有対象識別子Ｉｄｂ を含んでいる場合には、第１の設定要求Ｄｒｒａを受信したと、利用権管理部４１２は判断する。それに対して、共有対象識別子Ｉｄｂ を含んでいない場合には、後述する第２の設定要求Ｄｒｒ２ｂを受信したと、利用権管理部４１２は判断する。今回の場合、利用権管理部

４１２は、第１の設定要求Ｄｒｒａ を受信したと判断することになるから、ステップＳ１０２２を行う。

【０１７２】ステップＳ１０２２において、利用権管理部４１２は、受信した第１の設定要求Ｄｒｒａ から、機器識別子ＩｄＡ 、コンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ を取り出す。さらに、利用権管理部４１２は、利用権ＤＢ４１１にアクセスして、取り出したものを利用権レコードＲｒｇｔａとして登録する（ステップＳ１０２２）。ここで、第１の実施形態と同様に、利用条件Ｃｃｎｔ は、利用権情報Ｄｒｇｔとして使われる。以上のステップＳ１０２２により、利用権ＤＢ１１４は、図５２（ａ）に示すように、機器識別子ＩｄＡ および／または機器識別子ＩｄＢ、コンテンツ識別子Ｉｃｎｔ ならびに利用権情報Ｄｒｇｔ を含む利用権レコードＲｒｇｔａの集まりとなる。ところで、第１の実施形態では、図８のステップＳ１３２およびＳ１３３で説明したように、利用権管理部１１７は、機器２１ａ の設定要求Ｄｒｒａ の受信に応答して、ユーザ情報ＤＢ１１３から同一グループに属する全機器識別子ＩｄＡ およびＩｄＢ を取り出し、それらを全て利用権レコードＲｒｇｔ に登録していた。それに対して、第２の実施形態では、利用権管理部４１２は、ステップＳ１０２２の時点では、第１の設定要求Ｄｒｒａ の送信元となる機器識別子ＩｄＡのみを利用権レコードＲｒｇｔ に登録する。この点で、第１および第２の実施形態は顕著に相違する。

【０１７３】以上のステップＳ１０２２が終了すると、今回受け取った第１の設定要求Ｄｒｒａ を、利用権管理部４１２はコンテンツ管理部１１８に渡す。以降、利用権管理装置４１は、利用権管理装置１１と同様に、ステップＳ１４～Ｓ１７を実行し、その後、機器５１ａ は、機器２１ａ と同様に、ステップＳ１８～Ｓ１９を実行する。その結果、機器５１ａ は、利用権管理装置４１から、図９（ｂ）に示す形式を有する送信データＤｔｒｎａを受信する。また、本ライセンス情報管理システムＳｂ においても、機器５１ａ は、暗号済コンテンツデータＤｅｃｎｔを復号するために、ライセンス情報ＤＩｃａ（第１の実施形態参照）を利用権管理装置４１から受け取るが、この時の動作については第１の実施形態と同様であるため（図１１，図１２参照）、その説明を省略する。

【０１７４】また、機器５１ｂ が利用権管理装置４１に利用権レコードＲｒｇｔ の新規登録を要求する場合には、上述の機器５１ａ と利用権管理装置４１との間で行われたデータ通信と同様の動作が行われるので、その説明を省略する。

【０１７５】ユーザβは、機器５１ａ を使って、機器５１ｂ のために生成された利用権情報Ｄｒｇｔ を使いたい場合がある。このような場合、ユーザβは、機器５１ａ を操作して、コンテンツ識別子Ｉｃｎｔ を指定し、さらに、共有対象識別子ＩｄとしてのＩｄＢ を指定する。ここで注意を要するのは、機器５１ａ が、機器５１ｂ が既に設定した利用権情報Ｄｒｇｔ を共有することから、ユーザβは、利用条件Ｃｃｎｔ を特に指定する必要性が無い点である。以上の指定に応答して、機器５１ａ の設定要求生成部５１１は、今回指定されたものの中に、共有対象識別子ＩｄＢ が含まれているか否かを判断する（ステップＳ１０１）。上述から明らかなように、今回指定されるものには、共有対象識別子ＩｄＢ としての機器識別子ＩｄＢが含まれるので、設定要求生成部５１１は、図５３に示す第２の設定要求Ｄｒｒａを生成し、伝送路６１を通じて、利用権管理装置４１に送信する（ステップＳ１０３）。第２の設定要求Ｄｒｒａは、他の機器５１ｂ のために登録済の利用権情報Ｄｒｇｔ の共有設定を利用権管理装置４１に要求するための情報でもあり、本実施形態ではさらに、取得対象コンテンツデータＤｃｎｔ の配信を利用権管理装置４１に要求するための情報である。ステップＳ１０３をより具体的に説明すると、まず、設定要求生成部５１１は、機器識別子格納部２１１から機器識別子ＩｄＡ を受け取る。設定要求生成部５１１は、ユーザβが指定したコンテンツ識別子Ｉｃｎｔ および共有対象識別子ＩｄＢ に、取り出した機器識別子ＩｄＡ と、予め保持する設定要求識別子Ｉｒｒとを付加して、第２の設定要求Ｄｒｒ２ａ（図５３参照）を生成する。以上の第２の設定要求Ｄｒｒ２ａは、設定要求生成部５１１から通信部２１３および伝送路６１を通じて、利用権管理装置４１に送信される。

【０１７６】利用権管理装置４１（図４９参照）において、ユーザ認証部１１６は、伝送路６１からの第２の設定要求Ｄｒｒ２ａの受信に応答して、認証処理を行い（ステップＳ１１）、その後、受け取った第２の設定要求Ｄｒｒ２ａを利用権管理部４１２に渡す。利用権管理部４１２は、ユーザ認証部１１６から第２の設定要求Ｄｒｒ２ａを受信したことに応答して、利用権ＤＢ１１４への利用権登録処理を行う（ステップＳ１０２）。ステップＳ１０２において、利用権管理部４１２は、今回、第１の設定要求Ｄｒｒａ を受信したか否かを判断する（ステップＳ１０２１）。ここで、第２の設定要求Ｄｒｒ２ａには共有対象識別子ＩｄＢ が含まれるので、利用権管理部４１２は、第１の設定要求Ｄｒｒａ を受信していないと判断することになるから、ステップＳ１０２３を行う。

【０１７７】ステップＳ１０２３において、利用権管理部４１２は、受信した第２の設定要求Ｄｒｒ２ａから、共有対象識別子ＩｄＢ およびコンテンツ識別子Ｉｃｎｔ を取り出す。その後、利用権管理部４１２は、利用権ＤＢ４１１にアクセスして、取り出した共有対象識別子ＩｄＢ およびコンテンツ識別子Ｉｃｎｔ の双方を含む利用権レコードＲｒｇｔａを検索する。さらに、利用権管理部４１２は、受信した第２の設定要求Ｄｒｒ２ａから機器識別子ＩｄＡ を取り出し、検索した利用権レコードＲｒｇｔａに追加登録する（ステップＳ１０２４）。以上のステップＳ１０２４により、利用権ＤＢ１１４において、利用権レコードＲ

rgtaは、図５２（ｂ）に示すように、機器識別子Ｉdvaおよびｌdvb、コンテンツ識別子Ｉcnt ならびに利用権情報Drgt を含むものに更新される。これによって、コンテンツデータDcnt の利用権情報Drgtaは、機器５１a および５１b からなるサブグループにより共有されていることが示される。以上のステップＳ１０２５が終了すると、今回受け取った第２の設定要求Drr2aを、利用権管理部４１２はコンテンツ管理部１１８に渡す。以降、利用権管理装置４１は、ステップＳ１４～Ｓ１７を実行し、その後、機器５１b は、ステップＳ１８～Ｓ１９を実行する。また、本ライセンス情報管理システムＳb においても、機器５１a は、暗号済コンテンツデータDecntを復号するために、ライセンス情報Dlcb （第１の実施形態参照）を利用権管理装置４１から受け取る。この時、機器５１a および利用権管理装置４１では、第１の実施形態で機器２１b および利用権管理装置１１が行った処理と同様に、図１１および図１２に示す処理が行われる。

【０１７８】以上のように本実施形態によれば、利用権レコードRrgtaには、複数の機器識別子Ｉdva およびＩdvb が記録される。これによって、利用権管理装置４１は、互いに異なる機器５１a および５１b から発行要求Dira およびDirb が送信されてきたとしても、利用権レコードRrgtaを参照することで、同一の利用権情報Drgt から生成されたライセンス情報Dlca およびDlcbをそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【０１７９】さらに、第１の実施形態では、ユーザβが所有する複数の機器２１の１台が設定要求Drrを利用権管理装置１１に送信すれば、利用権管理装置１１は、そのユーザβが所有する全機器２１の機器識別子Ｉdvを権利レコードRrgt に一括的に登録していた。それに対して、本実施形態では、機器５１が第２の設定要求Drr2を送信しない限り、利用権管理装置４１は、その送信元の機器識別子Ｉdvを権利レコードRrgtaに登録しない。これによって、利用権情報Drgt の共有をより厳密に制御することが可能となる。

【０１８０】なお、以上の第２の実施形態に係るライセンス情報管理システムSb も、第１の実施形態に係るライセンス情報管理システムＳa と同様に、前述した第２～第５の変型例のような処理を利用権管理装置４１ならびに機器５１a および５１bに組み込むことで、機器識別子Ｉdva および／またはＩdvb の追加または削除が可能になる。

【０１８１】「第３の実施形態」図５４は、第３の実施形態に係るライセンス情報管理システムＳc の全体構成を示すブロック図である。図５４において、ライセンス情報管理システムＳc は、まず、少なくとも１つの利用権管理装置７１と、少なくとも１つの機器８１と、伝送路９１とを備えている。利用権管理装置７１は、コンテンツ配信に関わる事業者α側に設置される。また、機器８１は、事業者αとのユーザ契約に基づいてコンテンツ配信を受ける契約者β側に設置される。また、伝送路９１は、有線伝送路または無線伝送路であり、利用権管理装置７１および機器８１をデータ通信可能に接続する。

【０１８２】次に、図５５～図５８を参照して、図５４の利用権管理装置７１および機器８１の具体的な構成について説明する。図５５は、図５４の利用権管理装置７１の詳細な構成を示す機能ブロック図である。図５５において、利用権管理装置７１は、コンテンツデータベース７１１と、復号鍵データベース７１２と、ユーザ情報データベース７１３と、利用権データベース７１４と、通信部７１５と、ユーザ認証部７１６と、利用権管理部７１７と、コンテンツ管理部７１８と、コンテンツ暗号化部７１９と、送信データ生成部７２０と、ライセンス情報生成部７２１と、復号鍵管理部７２２と、復号鍵暗号化部７２３とを備えている。

【０１８３】また、図５６は、図５５のライセンス情報生成部７２１の詳細な構成を示す図である。図５６において、ライセンス情報生成部７２１は、ハッシュ値生成部７２１１と、ライセンス情報組立部７２１２とを含んでいる。

【０１８４】また、図５７は、図５４の機器８１の詳細な構成を示す機能ブロック図である。図５７において、機器８１は、従前の実施形態と同様の民生機器であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器８１は、機器識別子格納部８１１と、設定要求生成部８１２と、通信部８１３と、コンテンツ管理部８１４と、コンテンツ蓄積部８１５と、発行要求生成部８１６と、ライセンス情報処理部８１７と、コンテンツ復号部８１８と、コンテンツ再生部８１９とを備えている。

【０１８５】また、図５８は、図５７のライセンス情報処理部８１７の詳細な構成を示す機能ブロック図である。図５８において、ライセンス情報処理部８１７は、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。

【０１８６】次に、上記ライセンス情報管理システムＳc において、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、図５５のコンテンツデータベース（以下、コンテンツＤＢと称する）７１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）７１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢ）７１３とが構築される。

【０１８７】まず、図５９（ａ）を参照して、図５５のコンテンツＤＢ７１１について詳細に説明する。事業者αは、図５９（ａ）に示すようなコンテンツＤＢ７１１

を構築する。より具体的には、事業者αは、契約者βに提供すべきコンテンツデータＤcnt を、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータＤcnt は、機器８１で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータＤcnt は、ゲームプログラムまたはアプリケーションプログラムであっても良い。ただし、便宜上、本実施形態では、コンテンツデータＤcnt は音楽を表すデータであるとして、以下の説明を続ける。

【０１８８】事業者αは、以上のようにして得たコンテンツデータＤcnt のそれぞれに、コンテンツ識別子Ｉcnt を割り当てる。コンテンツ識別子Ｉcnt とは、本ライセンス情報管理システムＳc においてコンテンツデータＤcnt を一意に特定する。また、以上のコンテンツデータＤcnt は、デジタルライツを保護する観点から、利用権管理装置７１側で暗号化された上で機器８１に配信される。そのため、事業者αは、各コンテンツデータＤcnt に専用の暗号鍵Ｋe を割り当てる。以上のコンテンツ識別子Ｉcnt 、コンテンツデータＤcnt および暗号鍵Ｋe の組み合わせがコンテンツＤＢ７１１に蓄積される。したがって、図５９（ａ）に示すように、コンテンツＤＢ７１１は、コンテンツ識別子Ｉcnt 、コンテンツデータＤcntおよび暗号鍵Ｋe の組み合わせの集まりとなる。コンテンツＤＢ７１１において、コンテンツ識別子Ｉcnt は特に、同じ組みのコンテンツデータＤcnt を一意に特定する。また、暗号鍵Ｋe は、同じ組みのコンテンツデータＤcnt を暗号化するために使用される。

【０１８９】なお、以下の説明の便宜のため、図５９（ａ）に示す１つのコンテンツデータＤcnt には、一意なコンテンツ識別子Ｉcnt としての「ａ」が割り当てられると仮定する。さらに、コンテンツ識別子Ｉcnt としての「ａ」と同じ組みには、専用の暗号鍵Ｋe としての「ｂ」が登録されると仮定する。

【０１９０】また、本実施形態では、コンテンツＤＢ７１１は、コンテンツ識別子Ｉcnt 、コンテンツデータＤcnt および暗号鍵Ｋe から構成されるが、コンテンツデータＤcnt および暗号鍵Ｋe 毎のデータベースが構築されてもよい。また、コンテンツ識別子Ｉcnt は、コンテンツＤＢ７１１におけるコンテンツデータＤcnt の格納場所を特定する場合がある。かかる場合には、コンテンツＤＢ７１１に、コンテンツ識別子Ｉcnt を登録しておく必要性はない。つまり、コンテンツ識別子Ｉcnt は、コンテンツＤＢ７１１に必須の構成要素とならない。

【０１９１】次に、図５９（ｂ）を参照して、図５５の復号鍵ＤＢ７１２について詳細に説明する。上述したように、各コンテンツデータＤcnt は専用の暗号鍵Ｋe で暗号化された状態で機器８１に送信される。ここで、以下の説明において、暗号化されたコンテンツデータＤcnt を暗号済みコンテンツデータＤecntと称する。暗号済みコンテンツデータＤecntの復号のために、暗号鍵Ｋe に対応する復号鍵Ｋdが、機器８１に提供される必要がある。そのため、事業者αは、コンテンツＤＢ７１１内の各暗号鍵Ｋe に対応する復号鍵Ｋd を準備する。ここで、復号鍵Ｋdは、暗号鍵Ｋe と同じビット列からなっていてもよいし、異なるビット列からなっていてもよい。以上の復号鍵Ｋd は、上述のコンテンツ識別子Ｉcnt と共に、復号鍵ＤＢ７１２に蓄積される。以上のことから、復号鍵ＤＢ７１２は、図５９（ｂ）に示すように、コンテンツ識別子Ｉcnt および復号鍵Ｋd の組み合わせの集まりとなる。復号鍵ＤＢ７１２において、コンテンツ識別子Ｉcnt は特に、同じ組みの復号鍵Ｋd に割り当てられているコンテンツデータＤcnt を特定する。また、復号鍵Ｋd は、同じ組みのコンテンツ識別子Ｉcnt で特定される暗号済みコンテンツデータＤecntを復号するために使用される。

【０１９２】なお、以下の説明の便宜のため、図５９（ｂ）において、コンテンツ識別子Ｉcnt としての「ａ」と同じ組みには、復号鍵Ｋd として「ｃ」が登録されると仮定する。上述からも明らかであるが、復号鍵Ｋd としての「ｃ」は、暗号鍵Ｋeとしての「ｂ」による暗号済みコンテンツデータＤecntの復号に使用される。

【０１９３】次に、図６０（ａ）を参照して、図５５のユーザ情報ＤＢ７１３について詳細に説明する。上述の契約者βは、事業者αからコンテンツ配信を受けるために契約を交わす。ここで、両者の契約に関しては、契約者βが伝送路９１を通じて事業者αと行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者αは、契約者βに機器識別子Ｉdvを割り当てる。機器識別子Ｉdvは、ライセンス情報管理システムＳc において、契約者βの機器８１を一意に特定する。以上の機器識別子Ｉdvが、ユーザ情報ＤＢ７１３に登録される。以上のことから、図６０（ａ）に示すように、ユーザ情報ＤＢ７１３は、機器識別子Ｉdvの集まりとなる。

【０１９４】ここで図５７を再度参照する。図５７に示すように、事業者αにより割り当てられた機器識別子Ｉdvはさらに、契約者β側の機器８１における機器識別子格納部８１１に設定される。機器識別子Ｉdvの設定に関しては、典型的には、事業者αが契約者β側で管理される機器８１を操作して設定する。また、他にも、事業者α側が、伝送路９１を通じて、契約者βに割り当てた機器識別子Ｉdvを送信し、機器８１が、受信した機器識別子Ｉdvを機器識別子格納部８１１に自動的に登録するようにしてもよい。

【０１９５】なお、以上の機器識別子Ｉdvは、機器８１の工場出荷時に予め、機器識別子格納部８１１に設定されていてもよい。このような場合、契約者βは、事業者αのコンテンツ配信に加入する際に、機器８１に設定されている機器識別子Ｉdvを当該事業者αに告知する。そ

して、事業者αは、告知された機器識別子Ｉｄｖをユーザ情報ＤＢ７１３に登録する。

【０１９６】なお、以下の説明の便宜のため、図６０（ａ）に示すように、ユーザ情報ＤＢ７１３には、１つの機器識別子Ｉｄｖとして「ｘ１」が登録されると仮定する。また、図５７に示すように、機器識別子格納部８１１には、機器識別子Ｉｄｖとして「ｘ１」が設定されると仮定する。

【０１９７】ここで、図６０（ｂ）には、利用権データベース７１４が示されているが、当該利用権データベース７１４については、後で説明する。

【０１９８】以上の準備が終了すると、機器８１は、契約者βの操作に従って、利用権管理装置７１から、コンテンツデータＤｃｎｔ を取得することが可能となる。以下、図６１を参照して、コンテンツデータＤｃｎｔ の取得時における機器８１および利用権管理装置７１の動作について説明する。まず、契約者βは、機器８１を操作して、利用権管理装置７１にアクセスして、そのコンテンツＤＢ７１１に蓄積されているコンテンツデータＤｃｎｔ の中から、今回取得したいものコンテンツ識別子Ｉｃｎｔ を特定する。以降の説明において、今回指定されたコンテンツデータＤｃｎｔ を、取得対象コンテンツデータＤｃｎｔ と称する。さらに、契約者βは、取得対象コンテンツデータＤｃｎｔ を利用する際の利用条件Ｃｃｎｔ を指定する。

【０１９９】以下、利用条件Ｃｃｎｔ について、より詳細に説明する。利用条件Ｃｃｎｔ は、どのような条件で、機器８１がコンテンツデータＤｃｎｔ の利用権の設定を要求するのかを示す情報である。コンテンツデータＤｃｎｔ が音楽を表す場合、利用条件Ｃｃｎｔ としては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ｃｃｎｔ は、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、２つ以上の組み合わせであってもよい。利用条件Ｃｃｎｔ としての有効期間は、例えば、２００１年６月１日から２００１年８月３１日までと設定され、設定された期間に限り、機器８１は、コンテンツデータＤｃｎｔ を再生できる。再生回数は、例えば、５回と設定され、設定された回数に限り、機器８１は、コンテンツデータＤｃｎｔ を再生できる。最大連続再生時間は、例えば、１０秒と設定され、１回の再生において設定された時間までであれば、機器８１は、コンテンツデータＤｃｎｔ を再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、１０時間と設定され、設定された時間の範囲内であれば、機器８１は、コンテンツデータＤｃｎｔ を自由に再生できる。再生品質は、例えば、ＣＤ(CompactDisc)の品質と設定され、機器８１は、設定された再生品質でコンテンツデータＤｃｎｔ を再生できる。

【０２００】なお、上述では、コンテンツデータＤｃｎｔ が音楽を表す場合に設定されうる利用条件Ｃｃｎｔ について説明した。しかし、上述のみに限らず、利用条件Ｃｃｎｔ は、コンテンツデータＤｃｎｔ が表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ｃｃｎｔ は、コンテンツデータＤｃｎｔ の再生回数であるとして、以下の説明を続ける。

【０２０１】上述したように、契約者βは、機器８１を操作して、コンテンツ識別子Ｉｃｎｔおよび利用条件Ｃｃｎｔ を指定する。このような指定に応答して、機器８１は、図６２（ａ）に示す設定要求Ｄｒｒを生成し、利用権管理装置７１に送信する（図６１；ステップＳ２０１）。設定要求Ｄｒｒは、取得対象コンテンツデータＤｃｎｔ の利用権設定を利用権管理装置７１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤｃｎｔ の配信を利用権管理装置７１に要求するための情報でもある。ステップＳ２０１をより具体的に説明すると、まず、設定要求生成部８１２（図５７参照）は、契約者βが指定したコンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ を受け取る。また、設定要求生成部８１２は、機器識別子格納部８１１から機器識別子Ｉｄｖを受け取る。その後、設定要求生成部８１２は、以上の機器識別子Ｉｄｖ、コンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔに、予め保持する設定要求識別子Ｉｒｒを付加して、設定要求Ｄｒｒ（図６２（ａ）参照）を生成する。ここで、設定要求識別子Ｉｒｒは、利用権管理装置７１が設定要求Ｄｒｒを特定するために使用される。設定要求生成部８１２は、以上の設定要求Ｄｒｒを通信部８１３に渡す。通信部８１３は、受け取った設定要求Ｄｒｒを、伝送路９１を通じて、利用権管理装置７１に送信する。

【０２０２】利用権管理装置７１（図５５参照）において、通信部７１５は、伝送路９１を通じて送信されてくる設定要求Ｄｒｒを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、設定要求Ｄｒｒを受け取ると、ユーザ認証処理を行う（図６１；ステップＳ２０２）。より具体的には、ユーザ認証部７１６は、上述のユーザ情報ＤＢ７１３（図６０（ａ）参照）を管理しており、受け取った設定要求Ｄｒｒに設定されている機器識別子Ｉｄｖに一致するものが、当該ユーザ情報ＤＢ７１３に登録されているか否かを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回設定要求Ｄｒｒが、契約者βの機器８１から送信されてきたものであると判断する。ユーザ認証部７１６は、以上のユーザ認証が終了すると、受け取った設定要求Ｄｒｒを利用権管理部７１７に渡す。

【０２０３】なお、正規の契約者β以外からの設定要求Ｄｒｒを受け取った場合、ユーザ認証部７１６は、ユーザ認証に失敗する。かかる場合、ユーザ認証部７１６は、当該設定要求Ｄｒｒを利用権管理部７１７に渡すことなく、当該設定要求Ｄｒｒを廃棄する。

【０２０４】利用権管理部７１７（図５５参照）は、利

用権データベース（以下、利用権ＤＢと称する）７１４を管理している。また、利用権管理部７１７は、そこに設定されている設定要求識別子Ｉｒｒに基づいて、ユーザ認証部７１６から設定要求Ｄｒｒを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、利用権ＤＢ７１４への利用権登録処理を行う（ステップＳ２０３）。より具体的には、利用権管理部７１７は、設定要求Ｄｒｒから、機器識別子Ｉｄｖ、コンテンツ識別子Ｉｃｎｔ および利用条件Ｃｃｎｔ を取り出して、それらの組み合わせを利用権ＤＢ７１４に登録する。ここで、利用権管理部７１７は、設定要求Ｄｒｒに設定されている利用条件Ｃｃｎｔ で、機器８１が取得対象コンテンツデータＤｃｎｔ を利用する権利を要求しているとみなす。つまり、利用権管理部７１７からみれば、利用条件Ｃｃｎｔ は、取得対象コンテンツデータＤｃｎｔ を機器８１が利用できる権利を示す。以上の観点から、利用権管理部７１７は、設定要求Ｄｒｒから取り出した利用条件Ｃｃｎｔ を、機器８１が設定要求している利用権情報Ｄｒｇｔ として扱う。つまり、利用権ＤＢ７１４は、図６０（ｂ）に示すように、機器識別子Ｉｄｖ、コンテンツ識別子Ｉｃｎｔ および利用権情報Ｄｒｇｔ の組み合わせの集まりとなる。これによって、利用権管理部７１７は、契約者βｉ毎に、取得対象コンテンツデータＤｃｎｔ の利用権を管理する。利用権管理部７１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Ｄｒｒをコンテンツ管理部７１８に渡す。

【０２０５】ここで、以上の利用権ＤＢ７１４に登録される利用権情報Ｄｒｇｔ の具体例について説明する。既に説明している通り、本実施形態では、利用条件Ｃｃｎｔ は利用回数である仮定されている。さらに、今回の設定要求Ｄｒｒには、機器識別子Ｉｄｖとして「ｘ１」、コンテンツ識別子Ｉｃｎｔ として「ａ」および利用条件Ｃｃｎｔとして「再生ｍ回」（ｍは自然数）が設定されていると仮定する。以上の仮定下では、図６０（ｂ）に示すように、機器識別子Ｉｄｖとしての「ｘ１」、コンテンツ識別子Ｉｃｎｔ としての「ａ」および利用権情報Ｄｒｇｔ としての「再生ｍ回」の組み合わせが設定される。

【０２０６】なお、本ライセンス情報管理システムＳｃの技術的特徴とは関係ないが、ステップＳ２０３において、利用権管理部７１７は、利用権情報Ｄｒｇｔ の登録毎に、機器識別子Ｉｄｖが割り当てられている契約者βｉに対して課金を行ってもよい。

【０２０７】コンテンツ管理部７１８は、設定要求Ｄｒｒを受け取ると、コンテンツデータＤｃｎｔ の読み出し処理を行う（ステップＳ２０４）。より具体的には、コンテンツ管理部７１８は、受け取った設定要求Ｄｒｒから、コンテンツ識別子Ｉｃｎｔ を取り出す。その後、コンテンツ管理部７１８は、コンテンツＤＢ７１１にアクセスして、取り出したコンテンツ識別子Ｉｃｎｔ が割り当てられているコンテンツデータＤｃｎｔ および暗号鍵Ｋｅ を読み出す。以上の読み出し処理が終了すると、コンテンツ管理部７１８は、読み出したコンテンツデータＤｃｎｔ および暗号鍵Ｋｅ をコンテンツ暗号化部７１９に渡す。さらに、コンテンツ管理部７１８は、受け取った設定要求Ｄｒｒを送信データ生成部７２０に渡す。

【０２０８】コンテンツ暗号化部７１９は、コンテンツデータＤｃｎｔ の暗号処理を行う（ステップＳ２０５）。より具体的には、コンテンツ暗号化部７１９は、受け取ったコンテンツデータＤｃｎｔ を、それと同時に受け取った暗号鍵Ｋｅ で暗号化して、前述の暗号済みコンテンツデータＤｅｃｎｔを生成する。コンテンツ暗号化部７１９は、以上の暗号処理が終了すると、暗号済みコンテンツデータＤｅｃｎｔを送信データ生成部７２０に渡す。

【０２０９】送信データ生成部７２０は、コンテンツ管理部７１８からの設定要求Ｄｒｒと、コンテンツ暗号化部７１９からの暗号済みコンテンツデータＤｅｃｎｔとが揃うと、送信データ生成処理を行う（ステップＳ２０６）。より具体的には、送信データ生成部７２０は、受け取った設定要求Ｄｒｒから、コンテンツ識別子Ｉｃｎｔ を取り出す。さらに、送信データ生成部７２０は、取り出したコンテンツ識別子Ｉｃｎｔを、受け取った暗号済みコンテンツデータＤｅｃｎｔに付加して、図６２（ｂ）に示すような、送信データＤｔｒｎ を生成する。送信データ生成部７２０は、以上の送信データ生成処理が終了すると、送信データＤｔｒｎ を通信部７１５に渡す。通信部７１５は、受け取った送信データＤｔｒｎ を、伝送路９１を介して、機器８１へと送信する（ステップＳ２０７）。

【０２１０】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくる送信データＤｔｒｎ を受信する（ステップＳ２０８）。より具体的には、通信部８１３は、それに含まれるコンテンツ識別子Ｉｃｎｔ から、今回、送信データＤｔｒｎ を受信したことを認識する。このような認識結果に従って、通信部８１３は、受信データＤｔｒｎ をコンテンツ管理部８１４に渡す。

【０２１１】コンテンツ管理部８１４は、受信データＤｔｒｎ 内のコンテンツ識別子Ｉｃｎｔ および暗号済みコンテンツデータＤｅｃｎｔを、コンテンツ蓄積部８１５に蓄積する（ステップＳ２０９）。つまり、コンテンツ蓄積部８１５には、図６３に示すように、上述の設定要求Ｄｒｒにより要求されたコンテンツ識別子Ｉｃｎｔ および暗号済みコンテンツデータＤｅｃｎｔの組み合わせが、いくつか蓄積されることになる。

【０２１２】デジタルライツの保護の観点から、機器８１には暗号済みコンテンツデータＤｅｃｎｔが配信される。そのため、機器８１は、コンテンツデータＤｃｎｔ を利用する場合には、利用権管理装置７１により提供される復号鍵Ｋｄ で、暗号済みコンテンツデータＤｅｃｎｔを復号する必要がある。ここで、本ライセンス情報管理システムＳｃ では、復号鍵Ｋｄ を機器８１に提供するために、後

で詳説するライセンス情報Ｄｌｃが用いられる。以下、図６４～図６６を参照して、ライセンス情報Ｄｌｃの取得およびコンテンツデータＤｃｎｔ の復号時における機器８１および利用権管理装置７１の動作について説明する。

【０２１３】まず、契約者βは、機器８１を操作して、コンテンツ蓄積部８１５にアクセスして、そこに蓄積されている暗号済みコンテンツデータＤｅｃｎｔの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータＤｅｃｎｔを、復号対象コンテンツデータＤｅｃｎｔと称する。

【０２１４】以上の契約者βによる指定に応答して、機器８１は、図６７（ａ）に示すような発行要求Ｄｉｒを生成し、利用権管理装置７１に送信する（図６４；ステップＳ３０１）。発行要求Ｄｉｒは、上述のライセンス情報Ｄｌｃの提供を利用権管理装置７１に要求するため、つまり復号対象コンテンツデータＤｅｃｎｔの利用許可を受けるための情報である。より具体的にステップＳ３０１を説明すると、コンテンツ管理部８１４（図５７参照）は、コンテンツ蓄積部８１５を管理しており、契約者βにより特定された復号対象コンテンツデータＤｅｃｎｔに付加されているコンテンツ識別子Ｉｃｎｔ を、当該コンテンツ蓄積部８１５から取り出す。発行要求生成部８１６は、コンテンツ管理部８１４により取り出されたコンテンツ識別子Ｉｃｎｔ を受け取る。さらに、発行要求生成部８１６は、機器識別子格納部８１１から機器識別子Ｉｄｖを受け取る。その後、発行要求生成部８１６は、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔ に、発行要求識別子Ｉｉｒを付加して、発行要求Ｄｉｒ（図６７（ａ）参照）を生成する。ここで、発行要求識別子Ｉｉｒは、利用権管理装置７１が発行要求Ｄｉｒを特定するために使用される。発行要求生成部８１６は、以上の発行要求Ｄｉｒを通信部８１３に渡す。通信部８１３は、受け取った発行要求Ｄｉｒを伝送路９１を通じて、利用権管理装置７１に送信する。

【０２１５】利用権管理装置７１において、通信部７１５（図５５参照）は、伝送路９１を通じて送信されてくる発行要求Ｄｉｒを受信して、ユーザ認証部７１６に渡す。

【０２１６】ユーザ認証部７１６は、発行要求Ｄｉｒを受け取ると、ユーザ認証処理を行う（ステップＳ３０２）。より具体的には、ユーザ認証部７１６は、受け取った発行要求Ｄｉｒから、機器識別子Ｉｄｖを取り出す。この後、ユーザ認証部７１６は、ステップＳ２０２（図６１参照）と同様にして、今回の発行要求Ｄｉｒに認証処理を行った後に、当該発行要求Ｄｉｒを利用権管理部７１７に渡す。

【０２１７】利用権管理部７１７は、それに設定されている発行要求識別子Ｉｉｒに基づいて、今回、ユーザ認証部７１６から発行要求Ｄｉｒを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、受け取った発行要求Ｄｉｒから、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔ を取り出す（ステップＳ３０３）。次に、利用権管理部７１７は、取り出した機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されているか否かを判断する（ステップＳ３０４）。

【０２１８】利用権管理部７１７は、ステップＳ３０４で「Ｙｅｓ」と判断した場合、それらと同じ組みの利用権情報Ｄｒｇｔ を参照して、機器８１に利用許可を与えることができるか否かを判断する（ステップＳ３０５）。ステップＳ３０５で「Ｙｅｓ」と判断した場合、利用権管理部７１７は、利用権情報Ｄｒｇｔ の一部または全てを取り出す（ステップＳ３０６）。ここで、以下の説明において混同が生じることを避けるため、ステップＳ３０６において取り出された一部または全ての利用権情報Ｄｒｇｔ のことを、今回の発行要求Ｄｉｒにより特定される機器８１にコンテンツデータＤｃｎｔ の利用を許可するための情報であるという観点から、利用許可情報Ｄｌｗと称する。つまり、ステップＳ３０６では、利用許可情報Ｄｌｗが生成される。

【０２１９】利用許可情報Ｄｌｗの生成により、機器８１のために登録されている利用権情報Ｄｒｇｔ の一部または全てが使用される。そのため、ステップＳ３０６の次に、利用権管理部７１７は、ステップＳ３０６で一部または全部が取り出された利用権情報Ｄｒｇｔ を更新する（ステップＳ３０７）。

【０２２０】ここで、以上のステップＳ３０３～Ｓ３０７の処理の具体例について説明する。今、利用権ＤＢ７１４には、図６０（ｂ）に示すように、機器識別子Ｉｄｖとしての「ｘ１」、コンテンツ識別子Ｉｃｎｔ としての「ａ」および利用権情報Ｄｒｇｔとしての「再生ｍ回」の組みが登録されていると仮定する。また、今回、機器８１は、機器識別子Ｉｄｖとしての「ｘ１」およびコンテンツ識別子Ｉｃｎｔ としての「ａ」が設定されている発行要求Ｄｉｒを送信すると仮定する。

【０２２１】以上の仮定下では、ステップＳ３０３において、発行要求Ｄｉｒから、機器識別子Ｉｄｖとしての「ｘ１」と、コンテンツ識別子Ｉｃｎｔ としての「ａ」が取り出される。また、ステップＳ３０４において、機器識別子Ｉｄｖとしての「ｘ１」およびコンテンツ識別子Ｉｃｎｔ としての「ａ」の組みが、利用権ＤＢ７１４に登録されていると判断される。このように判断されると、ステップＳ３０５において、同じ組みの利用権情報Ｄｒｇｔ には、「再生ｍ回」と設定されているので、機器８１の利用許可を与えてもよいと判断される。このように判断されると、ステップＳ３０６において、利用許可情報Ｄｌｗが生成される。この時生成される利用許可情報Ｄｌｗとしては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のｍを超えない自然数であり、より好ましくは、機器８１の処理能力に応じて設定される。例えば、

機器８１が相対的に低い性能のハードウェアを搭載している場合であれば、ｎは、「１」のように、機器８１が復号対象コンテンツデータＤecntを利用可能な最低限の値に設定されることが好ましい。

【０２２２】以上のステップＳ３０３～Ｓ３０６により、機器８１（機器識別子Ｉｄｖ「ｘ１」）がコンテンツデータＤcnt（コンテンツ識別子Ｉcnt「ａ」）を再生する権利をｎ回使うことになる。そのため、ステップＳ３０７において、利用権情報Ｄrgtが「再生ｍ回」から「再生（ｍ－ｎ）回」に更新される。

【０２２３】以上の具体例では、利用権情報Ｄrgtがコンテンツデータ Ｄcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳｃでは、様々な利用権情報Ｄrgt（つまり利用条件Ｃcnｔ）を設定することができる。従って、ステップＳ３０３からＳ３０７までの処理手順は、利用権情報Ｄrgtに応じて適切に規定される必要がある。

【０２２４】以上のようにして生成した利用許可情報ＤＩｗを、利用権管理部７１７（図５５参照）は、発行要求Ｄirと一緒に、ライセンス情報生成部７２１に渡す。より具体的には、ライセンス情報生成部７２１は、図５６に示すように、ハッシュ値生成部７２１１およびライセンス情報組立部７２１２を含んでいる。ハッシュ値生成部７２１１には、利用許可情報ＤＩｗのみが渡され、また、ライセンス情報組立部７２１２には、利用許可情報ＤＩｗおよび発行要求Ｄirの双方が渡される。

【０２２５】まず、ハッシュ値生成部７２１１は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報ＤＩｗを代入して、利用許可情報ＤＩｗの改竄を防止するするためのハッシュ値Ｖhsを生成する（ステップＳ３０８）。つまり、ハッシュ値Ｖhsは、利用許可情報ＤＩｗを生成多項式ｆ（ｘ）に代入した時に得られる解である。以上のようなハッシュ値Ｖhsを、ハッシュ値生成部７２１１は、ライセンス情報組立部７２１２に渡す。

【０２２６】ライセンス情報組立部７２１２は、受け取った発行要求Ｄirを復号鍵管理部７２２に渡す。復号鍵管理部７２２（図５５参照）は、前述した復号鍵ＤＢ７１２（図５９（ｂ）参照）を管理する。復号鍵管理部７２２は、受け取った発行要求Ｄirに設定されているコンテンツ識別子Ｉcnt および機器識別子ＩｄｖをＤＢ７１２から取り出す。さらに、復号鍵管理部７２２は、コンテンツ識別子Ｉcnｔと同じ組みの復号鍵Ｋｄを復号鍵ＤＢ７１２から取り出して、機器識別子ＩｄｖとＩｃｎｔと一緒に復号鍵暗号化部７２３に渡す。復号鍵暗号化部７２３は、受け取った復号鍵Ｋｄを、同時に受け取った機器識別子Ｉｄｖで暗号化して（ステップＳ３０９）、暗号済みの復号鍵Ｋedを生成する。以上の暗号済み復号鍵Ｋedは、ライセンス情報組立部７２１２に渡される。

【０２２７】ライセンス情報組立部７２１２は、発行要求Ｄirおよび利用許可情報ＤＩｗ、ハッシュ値Ｖhsならびに暗号済み復号鍵Ｋedのすべてが揃うと、図６７（ｂ）に示すライセンス情報ＤＩcの生成を開始する（図６５；ステップＳ３０１０）。より具体的には、ライセンス情報組立部７２１２は、発行要求Ｄirから、コンテンツ識別子Ｉcnｔを取り出して、利用許可情報ＤＩｗ、暗号済み復号鍵Ｋedおよびハッシュ値Ｖhsに付加する。さらに、ライセンス情報組立部７２１２は、予め保持するライセンス情報識別子ＩＩcを、コンテンツ識別子Ｉcnｔに付加して、ライセンス情報ＤＩcを生成する。以上のライセンス情報ＤＩcは、復号対象コンテンツデータＤecntの機器８１における利用を制御するための情報である。また、ライセンス情報識別子ＩＩcは、機器８１がライセンス情報ＤＩcを特定するための情報である。また、以上のライセンス情報ＤＩcは、通信部７１５に渡される。通信部７１５から、伝送路９１を通じて、機器８１に送信される（ステップＳ３０１１）。

【０２２８】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくるライセンス情報ＤＩcを受信する（ステップＳ３０１２）。より具体的には、通信部８１３は、それに設定されるライセンス情報識別子ＩＩcから、今回、ライセンス情報ＤＩcを受け取ったことを認識する。このような認識結果に従って、通信部８１３は、受け取ったライセンス情報ＤＩcをライセンス情報処理部８１７に渡す。

【０２２９】ライセンス情報処理部８１７は、図５８に示すように、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。通信部８１３からのライセンス情報ＤＩcは、まず、改竄判定部８１７１に渡される。改竄判定部８１７１は、まず、受け取ったライセンス情報ＤＩcから、利用許可情報ＤＩwおよびハッシュ値Ｖhsを取り出し（ステップＳ３０１３）、取り出した利用許可情報ＤＩwを、ハッシュ値生成部８１７２に渡し、ハッシュ値Ｖhsをそのまま保持する。ここで、以下の説明において混同が生じないように、ステップＳ３０１３で取り出されたハッシュ値Ｖhsを、機器８１の外部（つまり利用権管理装置７１）で生成されたものであるという観点から、外部ハッシュ値Ｖehs と称する。

【０２３０】ハッシュ値生成部８１７２は、利用権管理装置７１側のハッシュ値生成部７２１１（図３参照）と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った利用許可情報ＤＩwをハッシュ関数ｆ（ｘ）に代入してハッシュ値Ｖhsを生成する（ステップＳ３０１４）。ここでステップＳ３０１４で生成されたハッシュ値Ｖhsを、機器８１の内部で生成されたものであるという観点から、内部ハッシュ値ＶＩhs と称する。ハッシュ値生成部８１７２は、以上の内部ハッシュ値ＶＩhs を、改竄判定部８１７１に返す。

【０２３１】改竄判定部８１７１は、上述の内部ハッシュ値ＶＩhs を受け取ると、利用許可情報ＤＩwが改竄され

ているか否かを判定する（ステップＳ３０１５）。より具体的には、上述の内部ハッシュ値Ｖｉｈｓ は、ライセンス情報ＤＩｃ内の利用許可情報ＤＩｗが改竄されていないという条件で、外部ハッシュ値Ｖｅｈｓ に一致する。そこで、ステップＳ３０１５において、改竄判定部８１７１は、受け取った内部ハッシュ値Ｖｉｈｓ が外部ハッシュ値Ｖｅｈｓ に一致するか否かを判定する。改竄判定部８１７１は、「Ｙｅｓ」と判定した場合には、利用許可情報ＤＩｗが改竄されておらず、今回送信されてきた利用許可情報ＤＩｗが有効であるとみなして、今回受け取ったライセンス情報ＤＩｃを利用許可判定部８１７３に渡す。

【０２３２】利用許可判定部８１７３は、受け取ったライセンス情報ＤＩｃを参照して、復号対象コンテンツデータＤｅｃｎｔの利用が許可されているか否かを判定する（ステップＳ３０１６）。利用許可判定部８１７３は、ステップＳ３０１６において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報ＤＩｃから、暗号済み復号鍵Ｋｅｄを取り出して、復号鍵復号部８１７４に渡す。

【０２３３】ここで、以上のステップＳ３０１６の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報ＤＩｃの利用許可情報ＤＩｗにより、コンテンツデータＤｃｎｔ の再生がｎ回だけ許可されている。かかる場合、利用許可判定部８１７３は、ステップＳ３０１６において、利用許可情報ＤＩｗに設定される再生回数ｍ１以上であれば、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていると判断して、受け取ったライセンス情報ＤＩｃから暗号済み復号鍵Ｋｅｄを取り出して、復号鍵復号部８１７４に渡す。

【０２３４】以上の具体例では、利用権情報Ｄｒｇｔ がコンテンツデータＤｃｎｔ の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳｃ では、様々な利用権情報Ｄｒｇｔ （つまり利用条件Ｃｃｎｔ ）を設定することができる。従って、ステップＳ３０１６の処理は、利用権情報Ｄｒｇｔ に応じて適切に規定される必要がある。

【０２３５】さて、復号鍵復号部８１７４は、利用許可判定部８１７３から暗号済み復号鍵Ｋｅｄを受け取る。さらに、復号鍵復号部８１７４は、機器識別子格納部８１１から機器識別子Ｉｄｖを受け取る。その後、復号鍵復号部８１７４は、暗号済み復号鍵Ｋｅｄを、機器識別子Ｉｄｖで復号して（ステップＳ３０１７）、復号鍵Ｋｄをコンテンツ復号部８１８に渡す。

【０２３６】ところで、コンテンツ管理部８１４は、ステップＳ３０１において、コンテンツ識別子Ｉｃｎｔ だけでなく、前述の復号対象コンテンツデータＤｅｃｎｔを取り出す。取り出された復号対象コンテンツデータＤｅｃｎｔ は、コンテンツ復号部８１８に渡される。コンテンツ復号部８１８は、復号鍵復号部８１７４から受け取った復号鍵Ｋｄで、復号対象コンテンツデータＤｅｃｎｔを復号して（ステップＳ３０１８）、コンテンツデータＤｃｎｔ をコンテンツ再生部８１９に渡す。コンテンツ再生部８１９は、受け取ったコンテンツデータＤｃｎｔ を再生して、音声出力する（ステップＳ３０１９）。これにより、契約者βは、事業者αから購入したコンテンツデータＤｃｎｔ が表す音楽を聴くことができる。

【０２３７】ここで、図６５のステップＳ３０１５を参照する。ステップＳ３０１５において、改竄判定部８１７１は、利用許可情報ＤＩｗが改竄されていると判定する場合がある。また、ステップＳ３０１６において、利用許可判定部８１７３は、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていないと判定する場合もある。このような場合、改竄判定部８１７１および利用許可判定部８１７３は、今回受け取ったライセンス情報ＤＩｃを破棄する（図６６；ステップＳ３０２０）。以上から明らかなように、本ライセンス情報管理システムＳｃ では、有効なライセンス情報ＤＩｃを受信した場合にのみ、復号対象コンテンツデータＤｅｃｎｔの復号が許可される。これによって、上述のデジタルライツが保護される。

【０２３８】ここで、図６４のステップＳ３０４において、利用権管理部７１７は、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ３０５において、利用権管理部７１７は、機器８１に利用許可を与えないと判断する場合もある。このような場合、利用権管理部７１７は、復号対象コンテンツデータＤｅｃｎｔの利用を拒否することを示す利用拒否情報Ｄｒｊ（図６７（ｃ）参照）を生成して、通信部７１５に渡す。通信部７１５は、受け取った利用拒否情報Ｄｒｊを、伝送路９１を介して、機器８１に送信する（図６６；ステップＳ３０２１）。

【０２３９】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくる利用拒否情報Ｄｒｊを受信する（ステップＳ３０２２）。利用拒否情報Ｄｒｊの受信以降、機器８１では何の処理も行われない。以上から明らかなように、本ライセンス情報管理システムＳｃ では、利用権ＤＢ７１４に有効な機器識別子Ｉｄｖ、コンテンツ識別子Ｉｃｎｔ および利用権情報Ｄｒｇｔ の組み合わせが登録されてない場合には、利用拒否情報Ｄｒｊが機器８１に送信される。これによって、機器８１側では、復号対象コンテンツデータＤｅｃｎｔは復号されない。これによって、上述のデジタルライツが保護される。

【０２４０】なお、ステップＳ３０４において、利用権管理部７１７は、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されていないと判断する場合、機器識別子Ｉｄｖ、コンテンツ識別子Ｉｃｎｔ および利用権情報Ｄｒｇｔ の組み合わせを新しく生成して、当該利用権ＤＢ７１４に登録するようにしてもよい。

【０２４１】以上説明したように、本ライセンス情報管

理システムＳｃ では、各コンテンツデータＤｃｎｔ を機器８１が利用するための権利を表す利用権情報Ｄｒｇｔ を利用権管理装置７１側で一元的に管理できるようになる。そのため、以上のような利用権情報Ｄｒｇｔ を管理するための処理負担を機器８１に負わせる必要がなくなる。これによって、本ライセンス情報管理システムＳｃ によれば、処理能力の低い民生機器に適した権利保護技術を提供することができる。

【０２４２】なお、以上の実施形態では、同じ事業者αにより管理される利用権管理装置７１が、図６１の処理および図６４～図６６の処理の双方を行うとして説明した。しかしながら、互いに異なる利用権管理装置が図６１の処理と図６４～図６６の処理とを行うようにしてもよい。つまり、ある事業者により管理される利用権管理装置がコンテンツデータＤｃｎｔ の配信を担当し、他の事業者により管理される利用権管理装置がライセンス情報Ｄｌｃの提供を担当するように、本ライセンス情報管理システムＳｃ は構成されてもよい。さらに、説明の便宜のため、本実施形態では、最初に、コンテンツデータＤｃｎｔ の取得（図６１の処理）が行われ、その後に、ライセンス情報Ｄｌｃの取得（図６４～図６６の処理）が行われていた。しかしながら、最初にライセンス情報Ｄｌｃの取得が行われ、その後に、コンテンツデータＤｃｎｔ の取得が行われても良い。また、コンテンツデータＤｃｎｔ の取得およびライセンス情報Ｄｌｃの取得が同時並行して行われてもよい。

【０２４３】また、以上の実施形態では、コンテンツＤＢ１１４は、暗号化されていないコンテンツデータＤｃｎｔ および暗号鍵Ｋｅ の集まりであった。利用権管理装置７１は、送信データＤｔｒｎ の生成直前に、コンテンツデータＤｃｎｔ を暗号鍵Ｋｅ で暗号化するようにしていた（ステップＳ２０５参照）。しかしながら、コンテンツデータＤｃｎｔ の暗号化に要する処理時間を削減するために、コンテンツＤＢ１１４は、前述の暗号済みコンテンツデータＤｅｃｎｔの集まりであってもよい。この場合、利用権管理装置７１は、設定要求Ｄｒｒに設定されるコンテンツ識別子Ｉｃｎｔが示す暗号済みコンテンツデータＤｅｃｎｔに、当該コンテンツ識別子Ｉｃｎｔ を付加して送信データＤｔｒｎ を生成し送信する。

【０２４４】また、以上の実施形態では、ライセンス情報生成部７２１において、ハッシュ値生成部７２１１は、利用許可情報Ｄｌｗのみからハッシュ値Ｖｈｓを生成していた。しかし、これに限らず、以下のようにしてハッシュ値Ｖｈｓを生成してもよい。まず、ライセンス情報組立部７２１２は、ライセンス情報Ｄｌｃの構成要素であるライセンス情報識別子ＩＩｃ、コンテンツ識別子Ｉｃｎｔ 、利用許可情報ＤＩｗ、および暗号済み復号鍵Ｋｅｄの内のいずれか、もしくは２つ以上をハッシュ値生成部７２１１に渡す。ハッシュ値生成部７２１１は、ライセンス情報組立部７２１２から受け取ったものを、上述のハッシュ関数ｆ（ｘ）に代入して、ハッシュ値Ｖｈｓを生成する。

【０２４５】また、以上の実施形態では、ライセンス情報ＤＩｃＩは、暗号済み復号鍵Ｋｅｄを含んでいた。しかし、これに限らず、ライセンス情報ＤＩｃＩは、復号鍵Ｋｄ を含んでいてもよい。この場合、伝送路９１上で、第三者に復号鍵Ｋｄ が盗まれる危険があるので、ＳＳＬ（Secure Socket Layer）に代表される技術を用いて、利用権管理装置７１から機器８１へと伝送されるライセンス情報ＤＩｃを保護することが好ましい。さらに、ＳＳＬだけでは、機器８１において、ライセンス情報ＤＩｃＩがそのままの状態で保持される。このような状況では、機器８１から他の機器へとライセンス情報ＤＩｃＩが転送されれば、当該他の機器は、ライセンス情報ＤＩｃを利用できるので、デジタルライツの保護という観点からは好ましくない。そのため、機器識別子格納部８１１に格納される機器識別子ＩｄのライセンスＤｌｃ情報ＤＩｃを暗号化するアルゴリズムを、機器８１に組み込むことがより好ましい。これにより、ライセンス情報ＤＩｃＩは機器８１以外では使用できなくなるので、デジタルライツを保護することが可能となる。

【０２４６】また、以上の実施形態では、説明の便宜上、ユーザ情報ＤＢ７１３には、機器識別子Ｉｄのみが登録されるとして説明した。しかしながら、ユーザ情報ＤＢ７１３にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。また、以上のような複雑なユーザ情報で復号鍵Ｋｄ を暗号化するようにしてもよい。これによって、復号鍵Ｋｄ の暗号強度が高くなるので、より好ましくデジタルライツを保護できるライセンス情報管理システムＳｃ を提供することが可能となる。

【０２４７】また、以上の実施形態では、説明の便宜上、コンテンツデータＤｃｎｔ が音楽データであるとして説明した。そのため、機器８１は、コンテンツ再生部８１９を含んでおり、当該コンテンツ再生部８１９は、復号されたコンテンツデータＤｃｎｔ を再生して、音声を出力するとして説明した。しかしながら、前述したように、コンテンツデータＤｃｎｔ は、機器８１で利用可能なデータであればよく、当該コンテンツデータＤｃｎｔ が表すのは、テレビ番組、映画、ラジオ番組、書籍、印刷物、ゲームプログラムまたはアプリケーションプログラム等、多岐にわたる。したがって、コンテンツ再生部８１９は、音声出力するものに限らず、コンテンツデータＤｃｎｔ の種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器８１は、以上のようなコンテンツ再生部８１９に代えて、復号されたコンテンツデータＤｃｎｔ を、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダ、ゲーム機器、ＰＣ、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインター

フェイスを備えていてもよい。

【０２４８】ところで、以上のライセンス情報管理システムＳｃ において、事業者αは、契約者βにコンテンツ配信を提供する。しかしながら、上述のライセンス情報管理システムＳｃ では、機器８１に機器識別子Ｉｄｖが固定的に設定されてしまうため、契約者βが、同じ事業者αと契約している宿泊施設において、自分の利用権情報Ｄｒｇｔ を使ってコンテンツデータＤｃｎｔ を、当該宿泊施設に設置された機器８１で利用することができないという問題点があった。また、同様の理由で、ある契約者βが、同じ事業者αと契約している知人宅において、自分の利用権情報Ｄｒｇｔ を使って、コンテンツデータＤｃｎｔ を利用することができないという問題点があった。以下の第６の変形例に係るライセンス情報管理システムＳｃ1は、以上のような問題点を解決して、より使い勝手のよいコンテンツ配信を実現することを目的とする。

【０２４９】「第６の変型例」図６８は、ライセンス情報管理システムＳｃ1の全体構成を示すブロック図である。図６８のライセンス情報管理システムＳｃ1は、図５４のライセンス情報管理システムＳｃ と比較すると、可搬型記録媒体１０１および機器２０１とをさらに備える点で相違する。この点以外に両システムＳｃ およびＳｃ1の間に構成面での相違は無いので、図６８において、図５４のライセンス情報管理システムＳｃ に相当する構成には同一の参照符号を付し、その説明を簡素化する。つまり、以下において、利用権管理装置７１および機器８１の説明を行う場合には、図５５～図５７を援用する。

【０２５０】可搬型記録媒体１０１は、代表的には、ＳＤカードやスマートメディア（いずれも商標）のように、契約者βが携帯可能な種類の記録媒体であって、図６９に示すように、自身を一意に特定するメディア識別子Ｉｍｄを、予め定められた記録領域に格納している。ここで、本実施形態では、便宜上、図６９に示すように、メディア識別子Ｉｍｄは「ｘ２」であるとして、以下の説明を続ける。以上の可搬型記録媒体１０１は、前述の機器８１と同じ契約者βにより管理される。

【０２５１】機器２０１は、事業者αとの契約に基づいてコンテンツ配信を受ける契約者γ側に設置される。ここで、契約者γは、本実施形態では、上述したような宿泊施設を所有しており、機器２０１は、当該宿泊施設に設置される。以下、機器２０１の詳細な構成を説明する。

【０２５２】ここで、図７０は、図６８の機器２０１の詳細な構成を示す機能ブロック図である。図７０において、機器２０１は、機器８１と同様の民生機器が代表的であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器２０１は、上述の可搬型記録媒体１０１を装着可能に構成されており、図５７に示す機器８１と比較すると、インターフェイス２０２１と、識別子抽出部２０２２とをさらに備える点で相違する。この点以外に両機器２０１および８１の間に構成面での相違は無いので、図７００機器２０１において、図５７の機器８１に相当する構成には同一の参照符号を付し、その説明を簡素化する。

【０２５３】次に、上記ライセンス情報管理システムＳｃ1において、契約者βが、自分の利用権情報Ｄｒｇｔ を使って、他者（つまり、契約者γ）側の機器２０１上で事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、前述の実施形態と同様に、まず、図５５のコンテンツデータベース（以下、コンテンツＤＢと称する）７１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）７１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢ）７１３とが構築される。なお、コンテンツＤＢ７１１および復号鍵ＤＢ７１２については、図５９（ａ）および同図（ｂ）を参照して前述した通りであるため、本変形例では、それぞれの説明を省略する。

【０２５４】しかしながら、ユーザ情報ＤＢ７１３には、前述の実施形態とは異なる情報の組み合わせが登録される。次に、図７１（ａ）を参照して、図５５のユーザ情報ＤＢ７１３について詳細に説明する。上述の契約者βは、事業者αからコンテンツ配信を受けるために契約を交わす。この契約に基づいて、事業者αは、契約者βにユーザ識別子Ｉｕｓｒ を割り当てる。ここで、ユーザ識別子Ｉｕｓｒ は、契約者βを一意に特定する。さらに、事業者αは、契約者βが管理する機器８１に、前述と同様の機器識別子Ｉｄｖを割り当てる。なお、上述の実施形態で説明したように、契約者βが、予め機器８１に設定されている機器識別子Ｉｄｖを事業者αに告知してもよい。機器識別子Ｉｄｖは、ライセンス情報管理システムＳｃ1において、契約者βの機器８１を一意に特定する。さらに、事業者αは、契約者βの可搬型記録媒体１０１に記録されているメディア識別子Ｉｍｄの告知を受ける。以上の機器識別子Ｉｄｖおよびメディア識別子Ｉｍｄの組み合わせが、契約者βのために、ユーザ識別子Ｉｕｓｒ と共に、ユーザ情報ＤＢ７１３に登録される。以上のことから、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３は、ユーザ識別子Ｉｕｓｒ 毎に登録される機器識別子Ｉｄｖおよびメディア識別子Ｉｍｄの組み合わせの集まりとなる。

【０２５５】また、前述の実施形態でも説明したように、事業者αにより割り当てられた機器識別子Ｉｄｖはさらに、契約者β側の機器８１における機器識別子格納部８１１に設定される（図５７参照）。

【０２５６】また、上述の契約者γも、事業者αからコンテンツ配信を受けるために契約を交わす。ここで、説明の便宜のため、契約者γは、契約者βとは異なり、可搬型記録媒体１０１を所有していないとする。以上の契約に基づいて、事業者αは、契約者γに、一意なユーザ

識別子Ｉusr を割り当てる。さらに、事業者αは、契約者γの機器２０１に、ライセンス情報管理システムＳc1において一意な機器識別子Ｉdvを割り当てる。以上の機器識別子Ｉdvが、契約者γのために、ユーザ情報ＤＢ７１３に、ユーザ識別子Ｉusr と共に登録される。以上のことから、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３は、ユーザ識別子Ｉusr 毎に登録される機器識別子Ｉdvの集まりとなる。

【０２５７】また、事業者αにより、機器２０１に割り当てられた機器識別子Ｉdvは、図７０に示すように、契約者γ側の機器２０１における機器識別子格納部８１１に設定される。

【０２５８】なお、以下の説明の便宜のため、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３には、契約者βのために、ユーザ識別子Ｉusr としての「ｙ１」に対応して、機器識別子Ｉdvとして「ｘ１」およびメディア識別子Ｉmdとして「ｘ２」が登録されると仮定する。この仮定下では、図５７に示すように、機器８１側の機器識別子格納部８１１には、機器識別子Ｉdvとして「ｘ１」が設定される。さらに、ユーザ情報ＤＢ７１３には、契約者γのために、ユーザ識別子Ｉusrとしての「ｙ２」に対応して、機器識別子Ｉdvとして「ｘ３」が登録されると仮定する。この仮定下では、図７０に示すように、機器２０１側の機器識別子格納部８１１には、機器識別子Ｉdvとして「ｘ３」が設定される。

【０２５９】ここで、図７１（ｂ）には、利用権データベース７１４が示されているが、当該利用権データベース７１４については、後で説明する。

【０２６０】以上の準備が終了すると、機器８１は、前述の実施形態で説明したように、利用権管理装置７１から、コンテンツデータＤcnt およびライセンス情報ＤＩc を取得することが可能となる（図６１，図６４～図６６参照）。さらに、本変形例の特徴的な点は、図６８に示すように、契約者βが可搬型記録媒体１０１を契約者γ側に持っていき、当該契約者γ側の機器２０１を使って、コンテンツデータＤcnt およびライセンス情報ＤＩc の提供を、利用権管理装置７１から受けることができる点である。

【０２６１】以下、図７２および図７３を参照して、契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作について説明する。まず、契約者βは、契約者γ側の機器２０１に、自分の可搬型記録媒体１０１を装着する。これによって、可搬型記録媒体１０１は、インターフェイス２０２１（図７０参照）を通じて、識別子抽出部２０２２とデータ通信可能に接続される。その後、契約者βは、機器２０１を操作して、利用権管理装置７１にアクセスして、そのコンテンツＤＢ７１１に蓄積されているコンテンツデータＤcnt の中から、今回取得したいもののコンテンツ識別子Ｉcnt を特定する。

以降の説明において、今回指定されたコンテンツデータＤcnt を、取得対象コンテンツデータＤcnt と称する。さらに、契約者βは、取得対象コンテンツデータＤcnt を利用する際の利用条件Ｃcnt を指定する。ここで、利用条件Ｃcnt については、前述の実施形態で詳しく説明しているので、ここではその説明を控える。また、本変形例においても、便宜上、利用条件Ｃcnt は、コンテンツデータＤcnt の再生回数であると仮定する。

【０２６２】上述したように、契約者βは、機器２０１を操作して、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を指定する。設定要求生成部８１２（図７０参照）は、契約者βが指定したコンテンツ識別子Ｉcnt および利用条件Ｃcnt を受け取る（ステップＳ４０１）。

【０２６３】次に、設定要求生成部８１２は、識別子抽出部２０２２に、機器識別子Ｉdvおよびメディア識別子Ｉmdのいずれか一方を選択して、自身に返すように指示する。ところで、可搬型記録媒体１０１が機器２０１に装着されている場合、当該機器２０１には、機器識別子格納部８１１に格納されている機器識別子Ｉdvと、可搬型記録媒体１０１に格納されているメディア識別子Ｉmdとが存在することになる。そのため、識別子抽出部２０２２は、設定要求生成部８１２の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子Ｉmdを取り出す。設定要求生成部８１２は、識別子抽出部２０２２により取り出されたメディア識別子Ｉmdを受け取る（ステップＳ４０２）。

【０２６４】ここで、識別子抽出部２０２２は、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子Ｉdvを取り出して、設定要求生成部８１２に渡すことになる。しかし、この場合、契約者γが、機器２０１を使って、コンテンツデータＤcnt の取得を行うこととなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子Ｉdvを取り出す場合における、機器２０１における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【０２６５】設定要求生成部８１２は、以上のメディア識別子Ｉmd、コンテンツ識別子Ｉcnt および利用条件Ｃcnt に、予め保持する設定要求識別子Ｉrrを付加して、設定要求Drr（図７４（ａ）参照）を生成する（ステップＳ４０３）。設定要求Drrは、取得対象コンテンツデータＤcnt の利用権設定を利用権管理装置７１１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤcnt の配信を利用権管理装置７１に要求するための情報である。また、設定要求識別子Ｉrrは、利用権管理装置７１が設定要求Drrを特定するために使用される。設定要求生成部８１２は、以上の設定

要求Drrを通信部８１３に渡す。通信部８１３は、受け取った設定要求Drrを、伝送路９１を通じて、利用権管理装置７１に送信する（ステップＳ４０４）。

【０２６６】利用権管理装置７１（図５５参照）において、通信部７１５は、伝送路９１を通じて送信されてくる設定要求Drrを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、設定要求Drrにユーザ認証処理を行う（ステップＳ４０５）。より具体的には、ユーザ認証部７１６は、上述のユーザ情報ＤＢ７１３（図７１（ａ）参照）を管理しており、受け取った設定要求Drrに設定されているメディア識別子 Imdに一致するものが、当該ユーザ情報ＤＢ７１３に登録されているか否かを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回設定要求Drrが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部７１６は、ユーザ情報ＤＢ７１３から、今回のメディア識別子 Imdに対応するユーザ識別子 Iusr を取り出して、受け取った設定要求Drrと共に利用権管理部７１７に渡す。

【０２６７】利用権管理部７１７（図５５参照）は、利用権データベース（以下、利用権ＤＢと称する）７１４を管理している。また、利用権管理部７１７は、そこに設定されている設定要求識別子 Irrに基づいて、ユーザ認証部７１６から設定要求Drrを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、利用権ＤＢ７１４への利用権登録処理を行う（ステップＳ４０６）。より具体的には、利用権管理部７１７は、設定要求Drrから、コンテンツ識別子 Icnt および利用条件 Ccnt を取り出して、それらと、受け取ったユーザ識別子 Iusr との組み合わせを利用権ＤＢ７１４に登録する。ここで、利用権管理部７１７は、設定要求Drrに設定されている利用条件 Ccnt で、契約者βが取得対象コンテンツデータ Dcnt を利用する権利の設定を要求しているとみなす。つまり、利用権管理部７１７からみれば、利用条件 Ccnt は、取得対象コンテンツデータ Dcnt を契約者βが利用できる権利を示す。以上の観点から、利用権管理部７１７は、設定要求Drrから取り出した利用条件 Ccnt を利用権情報 Drgt として扱う。つまり、利用権ＤＢ７１４は、図７１（ｂ）に示すように、ユーザ識別子 Iusr 、コンテンツ識別子 Icnt および利用権情報 Drgt の組み合わせの集まりとなる。これによって、利用権管理部７１７は、契約者βの取得対象コンテンツデータ Dcnt の利用権を管理する。利用権管理部７１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Drrをコンテンツ管理部７１８に渡す。

【０２６８】ここで、以上の利用権ＤＢ７１４に登録される利用権情報 Drgt の具体例について登録する。既に説明している通り、本実施形態では、利用条件 Ccnt は利用回数であると仮定されている。さらに、今回の設定要求Drrには、メディア識別子 Imdとして「ｘ１」、コンテンツ識別子 Icnt として「ａ」および利用条件 Ccnt として「再生m回」（mは自然数）が設定されていると仮定する。以上の仮定下では、ユーザ認証部７１６は、ステップＳ４０５のユーザ認証処理において、ユーザ識別子 Iusr としての「ｙ１」を、ユーザ情報ＤＢ７１３から取り出して、利用権管理部７１７に渡す。従って、ステップＳ４０６では、図７１（ｂ）に示すように、１つの利用条件情報 Dcrt には、ユーザ識別子 Iusr としての「ｙ１」、コンテンツ識別子 Icnt としての「ａ」および利用権情報 Drgt としての「再生m回」が設定される。

【０２６９】なお、本ライセンス情報管理システムＳｃ１の技術的特徴とは関係ないが、ステップＳ４０６において、利用権管理部７１７は、利用条件情報 Dcrt の登録毎に、ユーザ識別子 Iusr が割り当てられている契約者βに対して課金を行ってもよい。

【０２７０】コンテンツ管理部７１８は、設定要求Drrを受け取ると、図６１のステップＳ２０４と同様の読み出し処理を行う（ステップＳ４０７）。その後、コンテンツ暗号化部７１９は、ステップＳ２０５と同様の暗号処理を行う（ステップＳ４０８）。さらに、送信データ生成部７２０は、ステップＳ２０６と同様の送信データ生成処理を行う（ステップＳ４０９）。その結果、ステップＳ２０６と同様に、送信データ Dtrn （図６２（ｂ）参照）が、伝送路９１を介して、機器２０１へと送信される（ステップＳ４０１０）。

【０２７１】機器２０１（図７０参照）において、通信部８１３は、図６１のステップＳ２０８と同様の受信処理を行う（図７３；ステップＳ４０１１）。コンテンツ管理部８１４は、ステップＳ２０９と同様の蓄積処理を行う（ステップＳ４０１２）。その結果、コンテンツ蓄積部８１５には、図６３を参照して説明したように、コンテンツ識別子 Icnt および暗号済みコンテンツデータ Decntの組み合わせが、いくつか蓄積されることになる。

【０２７２】前述の実施形態での説明と同様に、機器２０１には暗号済みコンテンツデータ Decntが配信される。そのため、機器２０１は、コンテンツデータ Dcnt を利用する場合には、利用権管理装置７１により提供される復号鍵 Kd で、暗号済みコンテンツデータ Decntを復号する必要がある。ここで、本ライセンス情報管理システムＳｃ１では、復号鍵 Kd を、契約者βが操作中の機器２０１に提供するために、後で詳説するライセンス情報 Dlcが用いられる。以下、図７５～図７７を参照して、ライセンス情報 Dlcの取得およびコンテンツデータ Dcnt の復号時における機器２０１および利用権管理装置７１の動作について説明する。

【０２７３】まず、契約者βは、機器２０１を操作し

て、コンテンツ蓄積部８１５にアクセスして、そこに蓄積されている暗号済みコンテンツデータDecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータDecntを、復号対象コンテンツデータDecntと称する。

【０２７４】コンテンツ管理部８１４（図７０参照）は、コンテンツ蓄積部８１５を管理しており、契約者βにより特定された復号対象コンテンツデータDecntに付加されているコンテンツ識別子Icnt を、当該コンテンツ蓄積部８１５から取り出す。発行要求生成部８１６は、コンテンツ管理部８１４により取り出されたコンテンツ識別子Icnt を受け取る（ステップＳ５０１）。

【０２７５】次に、発行要求生成部８１６は、識別子抽出部２０２２に、機器識別子Idvおよびメディア識別子Imdのいずれか一方を選択して、自身に返すように指示する。識別子抽出部２０２２は、発行要求生成部８１６の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子Imdを取り出す。発行要求生成部８１６は、識別子抽出部２０２２により取り出されたメディア識別子Imdを受け取る（ステップＳ５０２）。

【０２７６】ここで、識別子抽出部２０２２は、前述したように、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子Idvを取り出して、設定要求生成部８１２に渡す。しかし、この場合、契約者βが、機器２０１を使って、ライセンス情報Dlcの提供を受けることとなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子Idvを取り出す場合における、機器２０１における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【０２７７】その後、発行要求生成部８１６は、メディア識別子ImdおよびコンテンツIdentifier Icnt に、発行要求識別子Iirを付加して、発行要求Dir（図７４（ｂ）参照）を生成する（ステップＳ５０３）。ここで、発行要求Dirは、上述のライセンス情報Dlcの提供を利用権管理装置７１に要求するための情報である。また、発行要求識別子Iirは、利用権管理装置７１が発行要求Dirを特定するために使用される。発行要求生成部８１６は、以上の発行要求Dirを通信部８１３に渡す。通信部８１３は、受け取った発行要求Dirを伝送路９１を通じて、利用権管理装置７１に送信する（ステップＳ５０４）。

【０２７８】利用権管理装置７１において、通信部７１５（図５５参照）は、伝送路９１を通じて送信されてくる発行要求Dirを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、発行要求Dirを受け取ると、ユーザ認証部７１６は、発行要求Dirにユーザ認証処理を行う（ステップＳ５０５）。より具体的には、ユーザ認証部７１６は、受け取った発行要求Dirに設定されているメディア識別子Imdに一致するものが、ユーザ情報ＤＢ７１３（図７１（ａ）参照）に登録されているかどうかを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回の発行要求Dirが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部７１６は、ユーザ情報ＤＢ７１３から、今回のメディア識別子Imdに対応するユーザ識別子Iusr を取り出して、受け取った発行要求Dirと共に利用権管理部７１７に渡す。

【０２７９】利用権管理部７１７は、発行要求Dirに設定されている発行要求識別子Iirに基づいて、今回、ユーザ認証部７１６から発行要求Dirを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、受け取った発行要求Dirからコンテンツ識別子Icnt を取り出す（ステップＳ５０６）。次に、利用権管理部７１７は、受け取ったユーザ識別子Iusr および取り出したコンテンツ識別子Icnt の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されているかどうかを判断する（ステップＳ５０７）。

【０２８０】利用権管理部７１７は、ステップＳ５０７で「Ｙｅｓ」と判断した場合、それらと同じ組みの利用権情報Drgt を参照して、契約者βが操作中の機器２０１に利用許可を与えることができるか否かを判断する（ステップＳ５０８）。ステップＳ５０８で「Ｙｅｓ」と判断した場合、利用権管理部７１７は、利用権情報Drgt の一部または全てを取り出す（ステップＳ５０９）。ここで、以下の説明において混同が生じることを避けるため、ステップＳ５０９において取り出された一部または全ての利用権情報Drgt のことを、今回の発行要求Dirにより特定される契約者βの機器２０１にコンテンツデータDcnt の利用を許可するための情報であるという観点から、利用許可情報Dlwと称する。つまり、ステップＳ５０９では、利用許可情報Dlwが生成される。

【０２８１】利用許可情報Dlwの生成により、契約者βのために登録されている利用権情報Drgt の一部または全てが使用される。そのため、ステップＳ５０９の次に、利用権管理部７１７は、ステップＳ５０９で一部または全部が取り出された利用権情報Drgt を更新する（図７５；ステップＳ５０１０）。

【０２８２】ここで、以上のステップＳ５０６～Ｓ５０１０の処理の具体例について説明する。今、利用権ＤＢ７１４には、図７１（ｂ）に示すように、ユーザ識別子Iusr としての「ｙ１」、コンテンツ識別子Icnt としての「ａ」および利用権情報Drgt としての「再生ｍ回」の組みが登録されていると仮定する。また、今回、機器２０１は、メディア識別子Imdとしての「ｘ２」お

よびコンテンツ識別子Ｉcnt としての「ａ」が設定されている発行要求Dirを送信すると仮定する。

【０２８３】以上の仮定下では、ステップＳ５０６において、利用権管理部７１７は、ユーザ識別子Ｉusr としての「ｙ１」を受け取り、さらに、発行要求Dirから、コンテンツ識別子Ｉcnt としての「ａ」を取り出す。また、ステップＳ５０７において、ユーザ識別子Ｉusr としての「ｙ１」およびコンテンツ識別子Ｉcnt としての「ａ」の組みが、利用権ＤＢ７１４に登録されていると判断される。このように判断されると、ステップＳ５０８において、同じ組みの利用権情報Drgt には、「再生m回」と設定されているので、契約者βが操作中の機器２０１の利用許可を与えてもよいと判断される。このように判断されると、ステップＳ５０９において、利用許可情報DIwが生成される。この時生成される利用許可情報DIwとしては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のmを超えない自然数であり、より好ましくは、機器２０１の処理能力に応じて設定される。例えば、機器２０１が相対的に低い性能のハードウエアを搭載している場合であれば、ｎは、「１」のように、機器２０１が復号対象コンテンツデータDecntを利用可能な最低限の値に設定することが好ましい。

【０２８４】以上のステップＳ５０６～Ｓ５０９により、機器２０１に装着された可搬型記録媒体１０１（メディア識別子Ｉmdが「ｘ２」）がコンテンツデータDcnt （コンテンツ識別子Ｉcnt 「ａ」）を再生する権利をｎ回使うことになる。そのため、ステップＳ５０１０において、契約者βの利用権情報Drgt が「再生m回」から「再生（ｍ－ｎ）回」に更新される。

【０２８５】以上のようにして生成した利用許可情報DIwを、利用権管理部７１７（図５５参照）は、発行要求Dirと一緒に、ライセンス情報生成部７２１に渡す。より具体的には、ライセンス情報生成部７２１は、図５６に示すように、ハッシュ値生成部７２１１およびライセンス情報組立部７２１２を含んでいる。ハッシュ値生成部７２１１には、利用許可情報DIwのみが渡され、また、ライセンス情報組立部７２１２には、利用許可情報DIwおよび発行要求Dirの双方が渡される。

【０２８６】まず、ハッシュ値生成部７２１１は、図６４のステップＳ３０８と同様にして、ハッシュ値Vhsを生成し（ステップＳ５０１１）、生成したハッシュ値Vhsをライセンス情報組立部７２１２に渡す。ライセンス情報組立部７２１２は、受け取った発行要求Dirを復号鍵管理部７２２に渡す。復号鍵管理部７２２（図５５参照）は、前述した復号鍵ＤＢ７１２（図５９（ｂ）参照）を管理する。復号鍵管理部７２２は、受け取った発行要求Dirに設定されているコンテンツ識別子Ｉcnt およびメディア識別子Ｉmdを取り出す。さらに、復号鍵管理部７２２は、コンテンツ識別子Ｉcnt と同じ組みの復号鍵Kd を復号鍵ＤＢ７１２から取り出して、メディア識別子Ｉmdと一緒に復号鍵暗号化部７２３に渡す。復号鍵暗号化部７２３は、受け取った復号鍵Kd を、同時に受け取ったメディア識別子Ｉmdで暗号化して（ステップＳ５０１２）、暗号済みの復号鍵Kedを生成する。以上の暗号済み復号鍵Kedは、ライセンス情報組立部７２１２に渡される。

【０２８７】ライセンス情報組立部７２１２は、発行要求Dirおよび利用許可情報DIw、ハッシュ値Vhsならびに暗号済み復号鍵Kedのすべてが揃うと、図６５のステップＳ３０１０と同様にして、図６７（ｂ）に示すライセンス情報DIcを生成する（ステップＳ５０１３）。以上のライセンス情報DIcは、通信部７１５に渡される。通信部７１５から、伝送路９１を通じて、機器２０１に送信される（ステップＳ５０１４）。

【０２８８】機器２０１（図７０参照）において、通信部８１３は、ステップＳ３０１２と同様にして、伝送路９１を通じて送信されてくるライセンス情報DIcを受信し（ステップＳ５０１５）、ライセンス情報処理部８１７に渡す。

【０２８９】ライセンス情報処理部８１７は、図５８に示すように、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。通信部８１３からのライセンス情報DIcは、まず、改竄判定部８１７１に渡される。改竄判定部８１７１は、まず、ステップＳ３０１３と同様に、受け取ったライセンス情報DIcから、利用許可情報DIwを取り出し、さらに、ハッシュ値Vhsを外部ハッシュ値Vehs として取り出し（ステップＳ５０１６）、取り出した利用許可情報DIwを、ハッシュ値生成部８１７２に渡し、外部ハッシュ値Vehs をそのまま保持する。

【０２９０】ハッシュ値生成部８１７２は、ステップＳ３０１４と同様にして、内部ハッシュ値Vlhs を生成して（ステップＳ５０１７）、改竄判定部８１７１に返す。

【０２９１】改竄判定部８１７１は、上述の内部ハッシュ値Vlhs を受け取ると、ステップＳ３０１５と同様にして、利用許可情報DIwが改竄されているか否かを判定し（ステップＳ５０１８）、「Ｙｅｓ」と判定した場合には、今回受け取ったライセンス情報DIcを利用許可判定部８１７３に渡す。

【０２９２】利用許可判定部８１７３は、受け取ったライセンス情報DIcを参照して、ステップＳ３０１６と同様にして、復号対象コンテンツデータDecntの利用が許可されているか否かを判定する（ステップＳ５０１９）。利用許可判定部８１７３は、ステップＳ５０１９において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報DIcから、暗号済み復号鍵Kedを取り出して、復号鍵復号部８１７４に渡す。

【０２９３】ここで、以上のステップＳ５０１９の処理

の具体例について説明する。前述の仮定に従えば、今回のライセンス情報ＤＩｃの利用許可情報ＤＩｗにより、コンテンツデータＤｃｎｔ の再生がｎ回だけ許可されている。かかる場合、利用許可判定部８１７３は、ステップＳ５０１９において、利用許可情報ＤＩｗに設定される再生回数が１以上であれば、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていると判断して、受け取ったライセンス情報ＤＩｃから暗号済み復号鍵Ｋｅｄを取り出して、復号鍵復号部８１７４に渡す。

【０２９４】さて、復号鍵復号部８１７４は、利用許可判定部８１７３から暗号済み復号鍵Ｋｅｄを受け取る。さらに、復号鍵復号部８１７４は、識別子抽出部２０２２に、機器識別子Ｉｄおよびメディア識別子Ｉｍｄのいずれか一方を選択して、自身に返すように指示する。識別子抽出部２０２２は、復号鍵復号部８１７４の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子Ｉｍｄを取り出す。復号鍵復号部８１７４は、識別子抽出部２０２２により取り出されたメディア識別子Ｉｍｄを受け取る。

【０２９５】ここで、識別子抽出部２０２２は、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子Ｉｄｖを取り出して、復号鍵復号部８１７４に渡すことになる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子Ｉｄｖを取り出す場合における、機器２０１における動作については、前述の実施形態と同様であるため、その説明を省略する。

【０２９６】以上のようにして、メディア識別子Ｉｍｄを受け取ると、復号鍵復号部８１７４は、暗号済み復号鍵Ｋｅｄを、メディア識別子Ｉｍｄで復号して（図７７；ステップＳ５０２０）、復号鍵Ｋｄ をコンテンツ復号部８１８に渡す。

【０２９７】ところで、コンテンツ管理部８１４は、ステップＳ５０１において、コンテンツ識別子Ｉｃｎｔ だけでなく、前述の復号対象コンテンツデータＤｅｃｎｔを取り出す。取り出された復号対象コンテンツデータＤｅｃｎｔ は、コンテンツ復号部８１８に渡される。コンテンツ復号部８１８は、復号鍵復号部８１７４から受け取った復号鍵Ｋｄ で、復号対象コンテンツデータＤｅｃｎｔを復号して（ステップＳ５０２１）、コンテンツデータＤｃｎｔ をコンテンツ再生部８１９に渡す。コンテンツ再生部８１９は、受け取ったコンテンツデータＤｃｎｔ を再生して、音声出力する（ステップＳ５０２２）。これにより、契約者βは、事業者αから購入したコンテンツデータＤｃｎｔ が表す音楽を聴くことができる。以上説明したように、本ライセンス情報管理システムＳｃ１によれば、契約者βは、自分が得た利用権情報Ｄｒｇｔを使って、別の契約者γが管理する機器２０１で、コンテンツデータＤｃｎｔ を利用することが可能となる。これによって、より使い勝手のよいライセンス情報管理システムＳｃ１を提供することが可能となる。

【０２９８】ここで、図７６のステップＳ５０１８において、改竄判定部８１７１は、利用許可情報ＤＩｗが改竄されていると判定する場合がある。また、ステップＳ５０１９において、利用許可判定部８１７３は、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていないと判定する場合もある。このような場合、改竄判定部８１７１および利用許可判定部８１７３は、図６６のステップＳ３０２０を実行して、今回受け取ったライセンス情報ＤＩｃを破棄する。

【０２９９】また、図７５のステップＳ５０７において、利用権管理部７１７は、ユーザ識別子Ｉｕｓｒ およびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ５０８において、利用権管理部７１７は、契約者βが操作中の機器２０１に利用許可を与えないと判断する場合もある。このような場合、利用権管理部７１７は、図６６のステップＳ３０２１を実行して、利用拒否情報Ｄｒｊを生成して、通信部７１５に渡す。通信部７１５は、受け取った利用拒否情報Ｄｒｊを、伝送路９１を介して、機器２０１に送信する。これによって、前述の実施形態と同様に、機器２０１が、復号対象コンテンツデータＤｅｃｎｔを復号しないようにすることができる。

【０３００】なお、ステップＳ５０７において、利用権管理部７１７は、ユーザ識別子Ｉｕｓｒ およびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されていないと判断する場合に、ユーザ識別子Ｉｕｓｒ 、コンテンツ識別子Ｉｃｎｔ および利用権情報Ｄｒｇｔ を生成して、利用権ＤＢ７１４に登録するようにしてもよい。

【０３０１】なお、以上の変形例において、契約者β側には、前述の実施形態で説明した機器８１が設置されるとして説明したが、これに限らず、上述の機器２０１が設置されてもよい。

【０３０２】また、以上の変形例において、機器２０１は、機器識別子格納部８１１を備えるとして説明した。しかしながら、契約者γ自身が機器２０１を使ってコンテンツデータＤｃｎｔ およびライセンス情報ＤＩｃの提供を利用権管理装置７１から受けない場合には、機器２０１は、機器識別子格納部８１１を備える必要性はない。

【０３０３】また、以上の変形例においても、前述の実施形態と同様に、互いに異なる利用権管理装置７２および図７３の処理と図７５～図７７の処理とを行うようにしてもよい。さらに、本変形例においても、最初にライセンス情報ＤＩｃの取得が行われ、その後に、コンテンツデータＤｃｎｔ の取得が行われても良い。また、コンテンツデータＤｃｎｔ の取得およびライセンス情報ＤＩｃの

取得が同時並行して行われてもよい。

【０３０４】また、以上の変形例では、説明の便宜上、ユーザ情報ＤＢ７１３には、ユーザ識別子Ｉusr と、機器識別子Ｉdvおよび／またはメディア識別子Ｉmdが登録されるとして説明した。しかしながら、前述の実施形態と同様に、ユーザ情報ＤＢ７１３にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。

【０３０５】また、以上の変形例は、前述の実施形態と同様、機器２０１におけるコンテンツ再生部８１９は、コンテンツデータＤcnt の種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器２０１は、以上のようなコンテンツ再生部８１９に代えて、復号されたコンテンツデータＤcnt を、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダ、ゲーム機器、ＰＣ、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインターフェイスを備えていてもよい。

【０３０６】また、以上の変形例においても、前述の実施形態と同様、ＳＳＬ等の保護技術を適用するという条件で、ライセンス情報ＤＩcは、暗号化されていない復号鍵Ｋd をそのまま含んでいてもよい。また、デジタルライツを保護するために、機器２０１には、可搬型記録媒体１０１に格納されるメディア識別子Ｉmdでライセンス情報ＤＩcを暗号化するアルゴリズムが組み込まれることがより好ましい。

【０３０７】また、以上の第６の変型例に係るインターフェイス２０２１および識別子抽出部２０２２は、第２の実施形態に係る機器５１に組み込まれても良い。このように、機器５１a または５１b に、インターフェイス２０２１および識別子抽出部２０２２の両者を組み込んだ場合、識別子抽出部２０２２は、ユーザの指定に従って、機器５１a または５１b の機器識別子格納部２１１に設定されている機器識別子Ｉdva またはＩdvb もしくは、可搬型記録媒体１０１に格納されているメディア識別子Ｉmdのいずれかを使って、設定要求Drr を生成して、利用権管理装置４１に送信する。これによって、ユーザは、機器５１a または５１b もしくは可搬型記録媒体１０１のいずれかを使って、コンテンツデータＤcnt を利用できるようになるので、より使い勝手の良いライセンス情報管理システムＳb を実現できるようになる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る利用権管理装置１１を収容したライセンス情報管理システムＳa の全体構成を示すブロック図である。

【図２】図１の利用権管理装置１１の詳細な構成を示すブロック図である。

【図３】図２のライセンス情報生成部１２１の詳細な構成を示すブロック図である。

【図４】図１の機器２１a および２１b の詳細な構成を示すブロック図である。

【図５】図４のライセンス情報処理部２１７の詳細な構成を示すブロック図である。

【図６】図２のコンテンツＤＢ１１１および図２の復号鍵ＤＢ１１２を示す模式図である。

【図７】図２のユーザ情報ＤＢ１１３および図２の利用権ＤＢ１１４を示す模式図である。

【図８】コンテンツデータＤcnt の利用権設定および取得時における、機器２１a および利用権管理装置１１の動作を示すフローチャートである。

【図９】図８に示す処理の過程で送受される設定要求Ｄrrおよび送信データＤtrn のフォーマットを示す模式図である。

【図１０】図４のコンテンツ蓄積部２１５に蓄積されるデータを示す模式図である。

【図１１】ライセンス情報ＤＩca の取得およびコンテンツデータＤcnt の復号時における機器２１a および利用権管理装置１１の動作を示す第１のフローチャートである。

【図１２】ライセンス情報ＤＩca の取得およびコンテンツデータＤcnt の復号時における機器２１a および利用権管理装置１１の動作を示す第２のフローチャートである。

【図１３】ライセンス情報ＤＩca の取得およびコンテンツデータＤcnt の復号時における機器２１a および利用権管理装置１１の動作を示す第３のフローチャートである。

【図１４】図１２～図１３の処理の過程で送受される発行要求Ｄir、ライセンス情報ＤＩcおよび利用拒否情報Ｄrjのフォーマットを示す模式図である。

【図１５】図１の利用権管理装置１１の第１の変型例に係る利用権管理装置１１a を収容したライセンス情報管理システムＳa1の全体構成を示すブロック図である。

【図１６】図１５に示す利用権管理装置１１a の詳細な構成を示すブロック図である。

【図１７】図１５に示す機器２１c の詳細な構成を示すブロック図である。

【図１８】図１５の機器２１c をユーザ情報ＤＢ１１３に登録するまでの機器２１c および利用権管理装置１１a の動作を示すフローチャートである。

【図１９】図１８の処理の過程で送受される登録要求Ｄrsc 、登録完了通知Ｄscc および登録拒否通知Ｄsrc のフォーマットを示す模式図である。

【図２０】図１８の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。

【図２１】図１の利用権管理装置１１の第２の変型例に係る利用権管理装置１１b の詳細な構成を示すブロック図である。

【図２２】第２の変型例に係る機器２１a または２１b

の詳細な構成を示すブロック図である。
【図２３】第２の変型例に係る機器２１ｃ の詳細な構成を示すブロック図である。
【図２４】機器２１ｃ の機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における機器２１ａ および利用権管理装置１１ｂ の動作を示すフローチャートである。
【図２５】機器２１ｃ の機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における機器２１ｃ および利用権管理装置１１ｂ の動作を示すフローチャートである。
【図２６】図２４の処理の過程で送受される仮登録要求Dprscおよび仮登録完了通知Dpsccのフォーマットを示す模式図である。
【図２７】図２４および図２５の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図２８】図２５の処理の過程で送受される本登録要求Dcrscおよび本登録完了通知Dcsccのフォーマットを示す模式図である。
【図２９】図１の利用権管理装置１１の第３の変型例に係る利用権管理装置１１ｃ の詳細な構成を示すブロック図である。
【図３０】第３の変型例に係る機器２１ａ または２１ｂ の詳細な構成を示すブロック図である。
【図３１】第３の変型例に係る機器２１ｃ の詳細な構成を示すブロック図である。
【図３２】機器２１ｃ の機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における、機器２１ｃ および利用権管理装置１１ｃ の動作を示すフローチャートである。
【図３３】機器２１ｃ の機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における、機器２１ａ および利用権管理装置１１ｃ の動作を示すフローチャートである。
【図３４】図３２の処理の過程で送受されるパスワード要求Drps およびパスワード通知Dpss のフォーマットを示す模式図である。
【図３５】図３２および図３３の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図３６】図３３の処理の過程で送受される登録要求Drsc および登録完了通知Dscc のフォーマットを示す模式図である。
【図３７】図１の利用権管理装置１１の第４の変型例に係る利用権管理装置１１ｄ の詳細な構成を示すブロック図である。
【図３８】第４の変型例に係る機器２１ａ または２１ｂ の詳細な構成を示すブロック図である。
【図３９】第４の変型例に係る機器２１ｃ の詳細な構成を示すブロック図である。
【図４０】機器２１ｃ の機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃ および利用権管理装置１１ｄ の動作を示すフローチャートである。
【図４１】図４０の処理の過程で送受される第１の登録要求Drsc1、第２の登録要求Drsc および登録完了通知Dscc のフォーマットを示す図である。
【図４２】図１の利用権管理装置１１の第５の変型例に係る利用権管理装置１１ｅ を収容したライセンス情報管理システムＳａ5の全体構成を示すブロック図である。
【図４３】図４２に示す利用権管理装置１１ｅ の詳細な構成を示すブロック図である。
【図４４】図４２に示す機器２１ｂ の詳細な構成を示すブロック図である。
【図４５】機器２１ｂ の機器識別子Ｉdvb をユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するまでの機器２１ｂ および利用権管理装置１１ｅ の動作を示すフローチャートである。
【図４６】図４５の処理の過程で送受される削除要求Drwb および削除完了通知Dswb のフォーマットを示す模式図である。
【図４７】図４５の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図４８】本発明の第２の実施形態に係る利用権管理装置４１を収容したライセンス情報管理システムＳb の全体構成を示すブロック図である。
【図４９】図４８の利用権管理装置４１の詳細な構成を示すブロック図である。
【図５０】図４８の機器５１ａ および５１ｂ の詳細な構成を示すブロック図である。
【図５１】コンテンツデータＤcnt の取得時における機器５１ａ および利用権管理装置４１の動作を示すフローチャートである。
【図５２】図４９の利用権ＤＢ１１４を示す模式図である。
【図５３】図５１の処理の過程で送受される第２の設定要求Drr2bのフォーマットを示す図である。
【図５４】本発明の第３の実施形態に係るライセンス情報管理システムＳc の全体構成を示すブロック図である。
【図５５】図５４の利用権管理装置７１の詳細な構成を示す機能ブロック図である。
【図５６】図５５のライセンス情報生成部７２１の詳細な構成を示す図である。
【図５７】図５４の機器８１の詳細な構成を示す機能ブロック図である。
【図５８】図５７のライセンス情報処理部８１７の詳細な構成を示す機能ブロック図である。
【図５９】図５５のコンテンツＤＢ７１１および図５５の復号鍵ＤＢ７１２を示す模式図である。
【図６０】図５５のユーザ情報ＤＢ７１３および利用権ＤＢ７１４を示す模式図である。
【図６１】コンテンツデータＤcnt の取得時における機

器８１および利用権管理装置７１の動作を示すフローチャートである。

【図６２】図６１の処理の過程で送受される設定要求Ｄrrおよび送信データＤtrn のフォーマットを示す模式図である。

【図６３】図５８のコンテンツ蓄積部８１５に格納されるデータを示す模式図である。

【図６４】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図６５】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図６６】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第３のフローチャートである。

【図６７】図６４～図６６の処理の過程で送受される発行要求Ｄir、ライセンス情報Ｄlcおよび利用拒否情報Ｄrjのフォーマットを示す模式図である。

【図６８】図５４のライセンス情報管理システムＳc の変型例に係るライセンス情報管理システムＳc1の全体構成を示すブロック図である。

【図６９】図６８の可搬型記録媒体１０１の構成を示す模式図である。

【図７０】図６８の機器２０１の詳細な構成を示す機能ブロック図である。

【図７１】図６８のユーザ情報ＤＢ７１３および利用権ＤＢ７１４を示す模式図である。

【図７２】契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図７３】契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図７４】図７２および図７３の処理の過程で送受される設定要求Ｄrrおよび発行要求Ｄirのフォーマットを示す模式図である。

【図７５】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図７６】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図７７】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第３のフローチャートである。

【符号の説明】

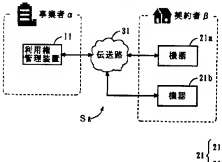
Ｓa，Ｓa1～Ｓa5，Ｓb，Ｓc，Ｓc1…ライセンス情報管理システム

１１，１１a～１１e，４１，７１…利用権管理装置

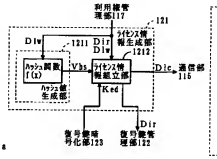
２１a～２１c，５１a，５１b，８１，２０１…機器

１０１…可搬型記録媒体

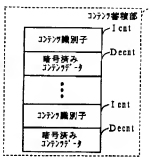
【図１】



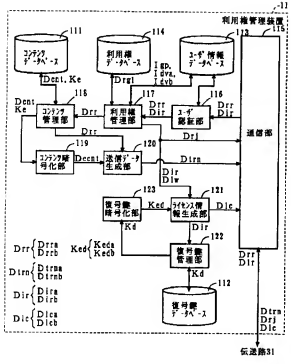
【図３】



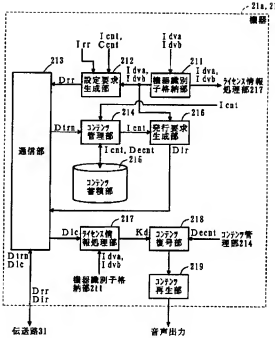
【図１０】



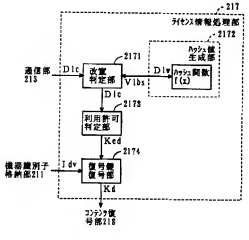
【図２】


利用権管理装置
コンテンツデータベース
利用履歴データベース
ユーザ情報データベース
Dcnt, Ke
コンテンツ管理部
利用履歴管理部
ユーザ認証部
通信部
コンテンツ暗号化部
送信データ生成部
復号鍵暗号化部
ライセンス情報生成部
復号鍵管理部
復号鍵データベース
伝送路31

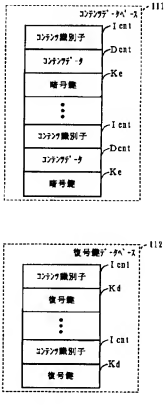
【図４】


機器
限定要求生成部
機器識別子格納部
ライセンス情報処理部217
コンテンツ管理部
発行要求生成部
通信部
コンテンツ蓄積部
ライセンス情報処理部
コンテンツ復号部
コンテンツ再生部
機器識別子格納部211
伝送路31
音声出力

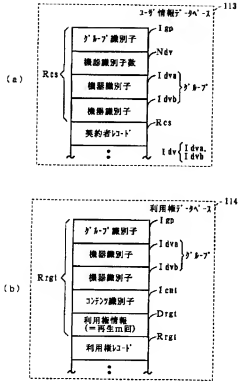
【図５】


ライセンス情報処理部
カウント値生成部
通信部
改竄判定部
利用許可判定部
復号鍵復号部
機器識別子格納部211
コンテンツ復号部218

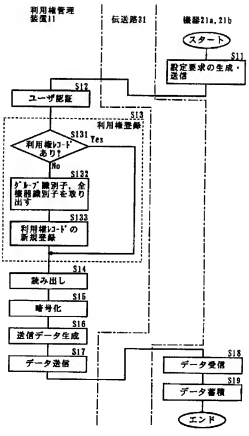
【図６】


(a)
(b)
コンテンツ識別子
コンテンツデータ
暗号鍵
復号鍵データベース
復号鍵

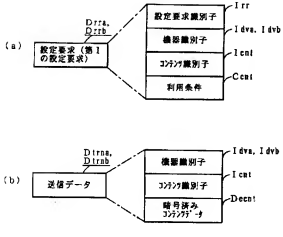
【図７】


ユーザ情報データベース
113
Igp
グループ識別子
Ndv
機器識別子数
Idva
Idvb
機器識別子
Rcs
契約者レコード
Idv
Idva, Idvb
(a)
利用権データベース
114
Igp
グループ識別子
Idva
Idvb
機器識別子
Icmt
コンテンツ識別子
Drgt
利用条件情報（＝再生回数）
Rrgt
利用権レコード
(b)

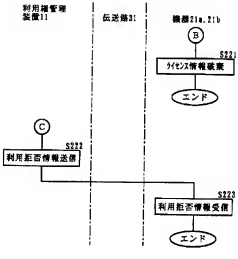
【図８】


利用権管理装置11
伝送路31
機器21a, 21b
スタート
S11
設定要求の生成・送信
S12
ユーザ認証
S13
利用権登録
S131
利用権レコードあり?
Yes
No
S132
グループ識別子、全機器識別子を取り出す
S133
利用権レコードの新規登録
S14
読み出し
S15
暗号化
S16
送信データ生成
S17
データ送信
S18
データ受信
S19
データ蓄積
エンド

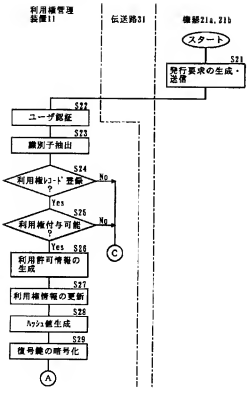
【図９】


(a)
Drra, Drrb
設定要求（第１の設定要求）
設定要求識別子
Irr
機器識別子
Idva, Idvb
コンテンツ識別子
Icmt
利用条件
Ccmt
(b)
Dtra, Dtrb
送信データ
機器識別子
Idva, Idvb
コンテンツ識別子
Icmt
暗号済みコンテンツデータ
Dccmt

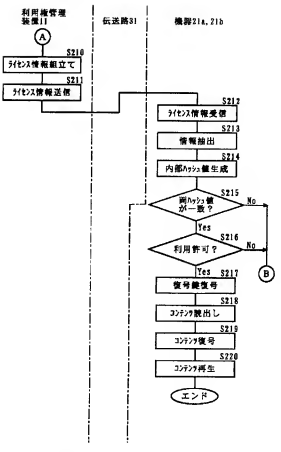
【図１３】


利用権管理装置11
伝送路31
機器21a, 21b
B
S221
ライセンス情報破棄
エンド
C
S222
利用拒否情報送信
S223
利用拒否情報受信
エンド

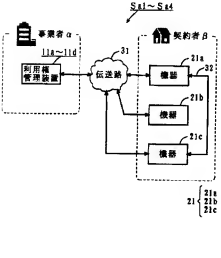
【図１１】



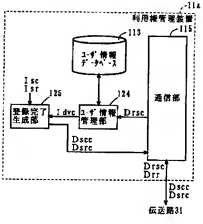
【図１２】



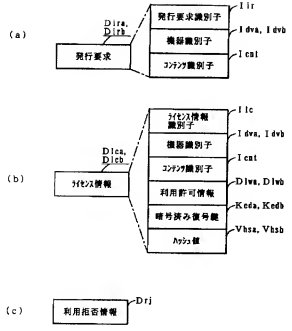
【図１５】



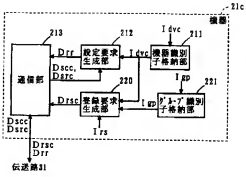
【図１６】



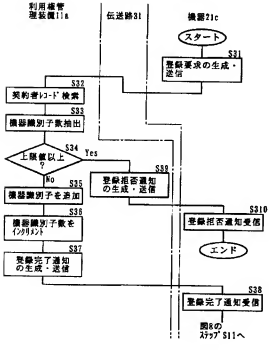
【図１４】



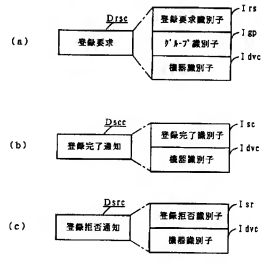
【図１７】



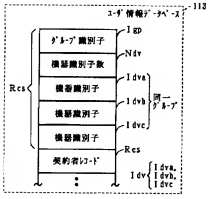
【図１８】



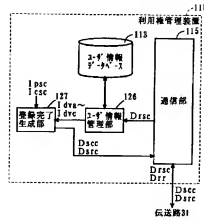
【図１９】



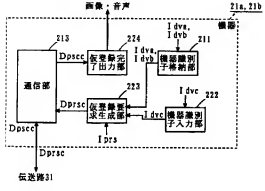
【図２０】



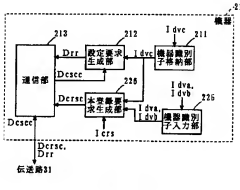
【図２１】



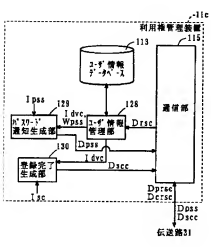
【図２２】



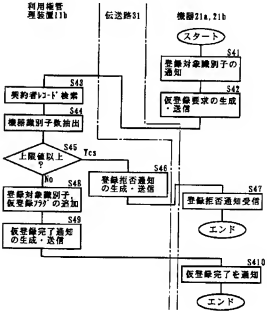
【図２３】



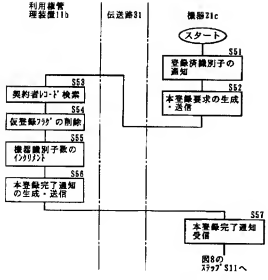
【図２９】



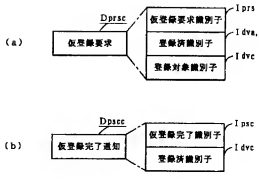
【図２４】



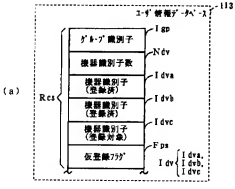
【図２５】

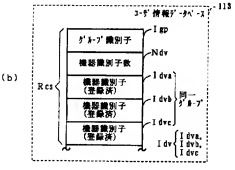


【図２６】

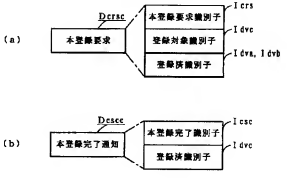


【図２７】

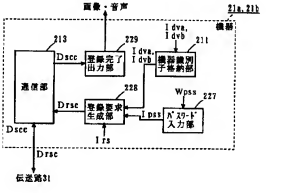




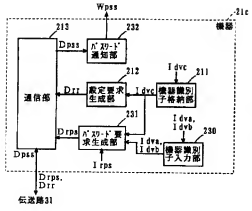
【図２８】



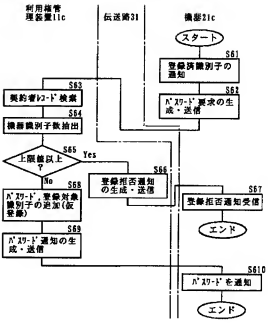
【図３０】



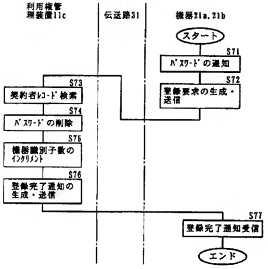
【図３１】



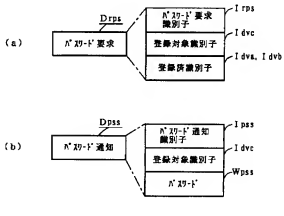
【図３２】



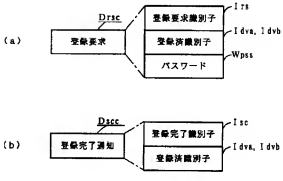
【図３３】



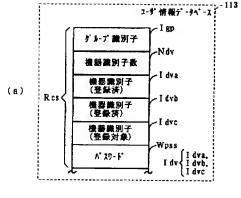
【図３４】



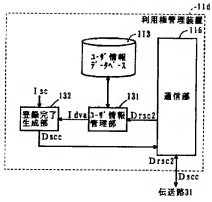
【図３６】



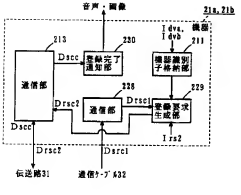
【図３５】



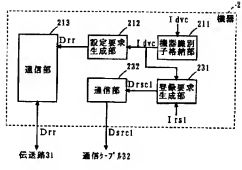
【図３７】



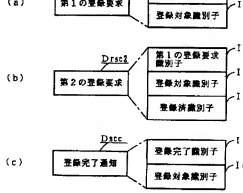
【図３８】



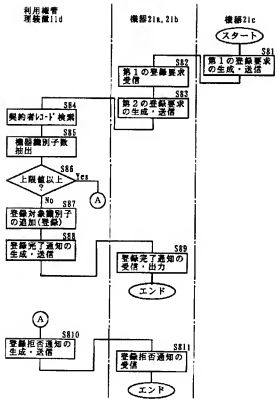
【図３９】



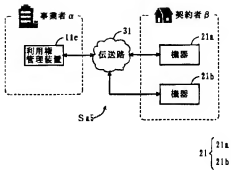
【図４１】



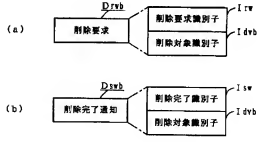
【図４０】



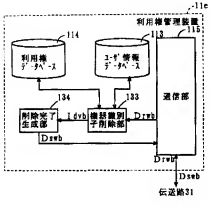
【図４２】



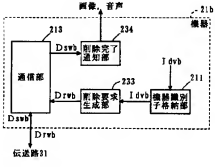
【図４６】



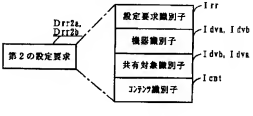
【図４３】



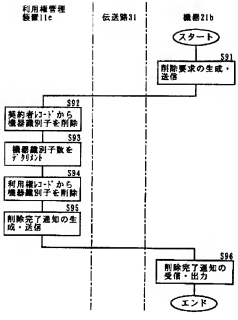
【図４４】



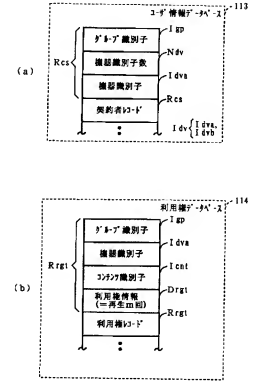
【図５３】



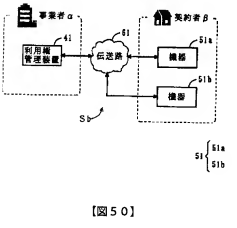
【図４５】



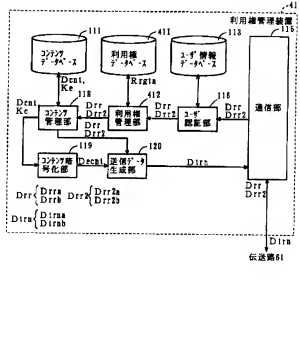
【図４７】



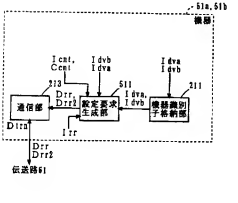
【図４８】



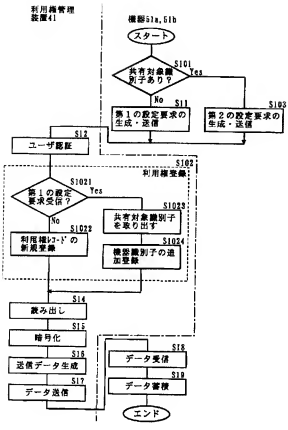
【図４９】



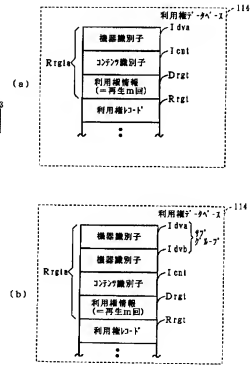
【図５０】



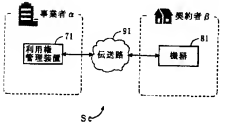
【図５１】



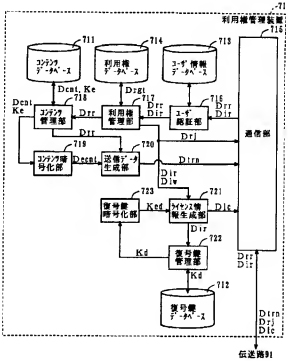
【図５２】



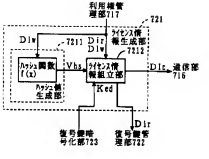
【図５３】



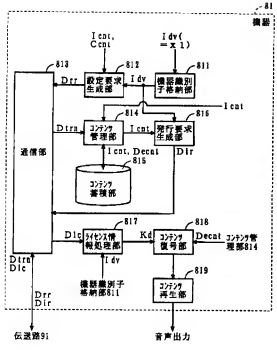
【図５４】



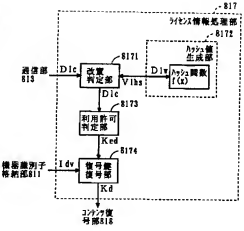
【図５６】



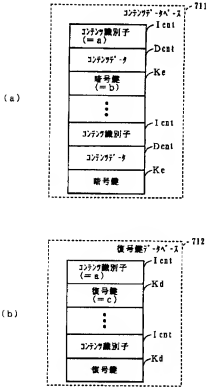
【図５７】



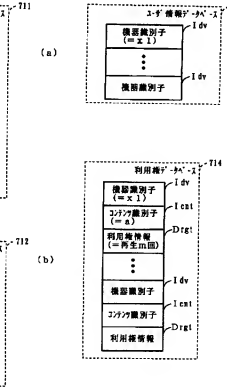
【図５８】



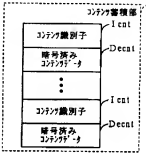
【図５９】



【図６０】

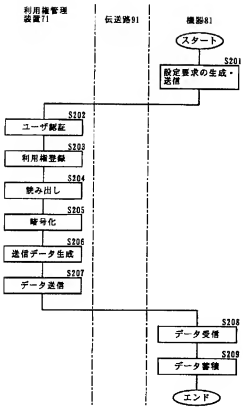


【図６３】

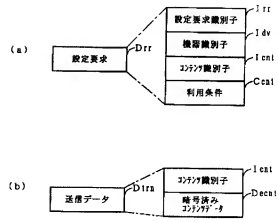


【図６９】

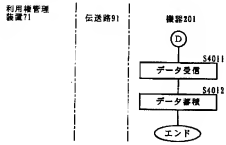
【図６１】



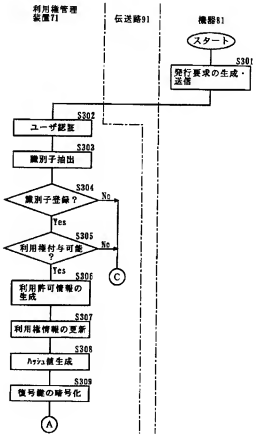
【図６２】



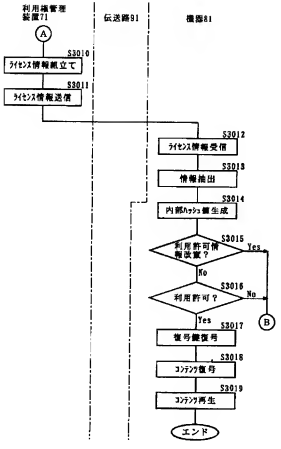
【図６３】



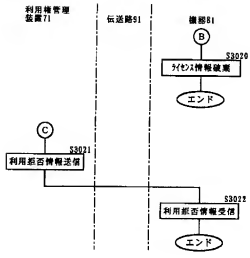
【図６４】



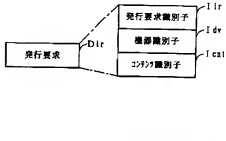
【図６５】



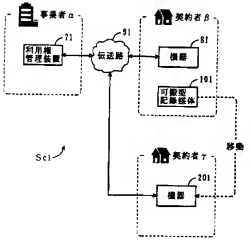
【図６６】



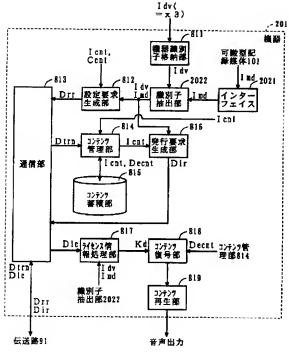
【図６７】



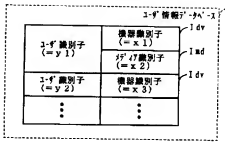
【図６８】



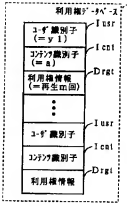
【図７０】



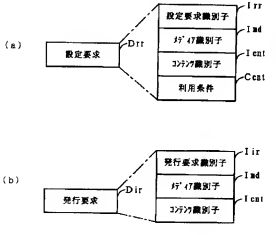
(a)



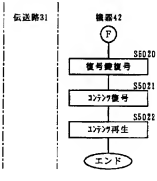
(b)



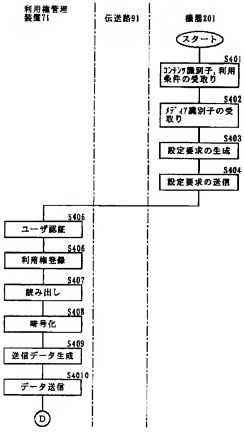
【図７４】



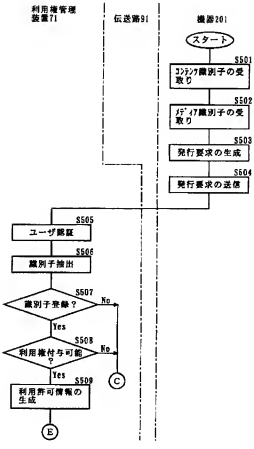
【図７７】



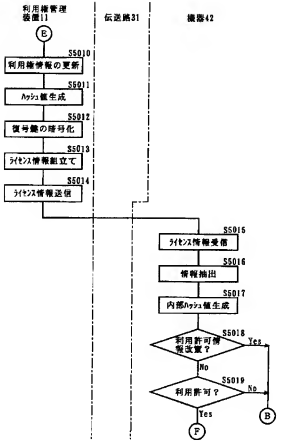
【図７２】


利用権管理装置71
伝送路91
機器201
スタート
S401
コンテンツ識別子，利用条件の受取り
S402
メディア識別子の受取り
S403
設定要求の生成
S404
設定要求の送信
S405
ユーザ認証
S406
利用権登録
S407
読み出し
S408
暗号化
S409
送信データ生成
S410
データ送信
D

【図７５】


利用権管理装置71
伝送路91
機器201
スタート
S501
コンテンツ識別子の受取り
S502
メディア識別子の受取り
S503
発行要求の生成
S504
発行要求の送信
S505
ユーザ認証
S506
識別子抽出
S507
識別子登録？
No
Yes
S508
利用権付与可能か？
No
Yes
S509
利用許可情報の生成
C
E

【図７６】



フロントページの続き

(51) Int. Cl.⁷　　識別記号　　F I　　テーマコード（参考）
H04L　9/08　　H04L　9/00　　601B
9/32　　673B

(72)発明者　山本　雅哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　岡本　隆一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　徳田　克己
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　井上　光啓
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Fターム(参考)　5B017 AA06 BB09 BB10 CA09 CA16
5B085 AE03 AE29 BA06 BG02 BG03 BG04 BG07
5J104 AA08 DA03 NA12 PA07 PA10